izzynobre ✓ 7 anos atrás

Mano, peloamordedeus, Bitcoin é uma piada na internet.

  RESPONDER

No futuro você se arrependerá amargamente de ter escrito isso.

Vamos ver quem vai rir por último.

- Daniel Fraga, em resposta a um comentário ironizando o bitcoin feito por izzynobre em 2013.

BITCOIN

Red Pill

O Renascimento Moral, Material e Tecnológico

— 2ª EDIÇÃO —

Renato Amoedo
Alan Schramm

ISBN: 979-8692311566

Agradecimento

Agradecemos a Cátia Regina Raulino, Eliezer de Queiroz Moreira, José Dirceu, Roger Abdelmassih, Eugenio Chipkevitch, Dilma Rousseff, João de Deus e Luiz Inácio, por mostrarem qual o comportamento dominante neste país e qual o nível moral de seus acadêmicos, instituições e dirigentes.

Sobre os autores

Renato Amoedo Nadier Rodrigues possui graduação em Engenharia de Produção Civil pela UNEB (2000-2006) - ocupando a 1ª posição no Enade 2006 - e graduação em Direito pela UFBA (2000-2004) - por aproveitamento extraordinário. Foi aprovado com nota máxima na Especialização em Direito Empresarial na UFBA (2004-2006) e laureado com nota máxima (10 com distinção) no Mestrado em Direito Privado e Econômico da UFBA (2005-2007). Foi Coordenador Adjunto do Curso de Direito da FBB e Professor desta instituição (2005-2007), da UNYAHNA (2006); da FTE (2007-2008); lecionou Direito Comercial como tirocinista, monitor e Professor substituto da UFBA (2008), aprovado em 1º lugar em seleção pública; e lecionou Direito Mercantil, Financeiro e Econômico como Professor Assistente na UFT (2008-2010), aprovado em 1º lugar no concurso público. Cursou o Doutorado em Administração (Finanças Estratégicas) da UPM - depositando tese sobre governança corporativa; assim como o *EMLE - European Master in Law and Economics* na condição de bolsista da Comissão Europeia pelo *"Erasmus Mundus Scholarship"* (1º lugar do mundo na seleção pela categoria A). É Perito Criminal desde 2007 e *bitcoiner* desde 2015.

Endereço para acessar este CV Lattes:
http://lattes.cnpq.br/6778421578122820

Alan Schramm de Lima cursou a *School of Art, Game and Animation SAGA* (2012-2014); possui graduação em Design de Comunicação Visual e Digital pela Universidade Salvador UNIFACS (2012-2016); *Higher Education Course em UX Design* pelo *Politecnico di Milano*-Itália (2019); Empreendedor na área do *Design* digital; Coautor de relatórios da INOVAFLIX (*Cryptoclub*) sobre Bitcoin (2018); Colunista do Portal Livecoins; Interesses por: Filosofia Libertária, Economia Austríaca, Cultura Digital, UI/UX *Design*, tecnologia e inovação.

Endereço para acessar este CV:
https://www.linkedin.com/in/alan-schramm-08878a57/

PATROCINADORES

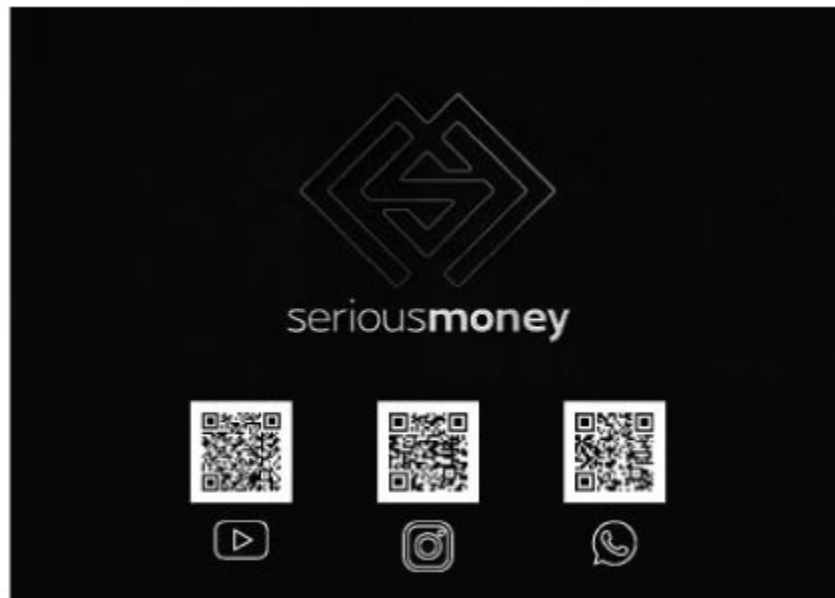
Agradecemos imensamente aos nossos patrocinadores
por apoiar este projeto de educação Bitcoin.

Esta edição contou com o patrocínio das seguintes empresas:

Acesse o site

www.stackbit.me

Acesse o site

www.p2ptrading.com.br

Estratégias para lucrar (ainda mais) com Bitcoin e Ethereum

- Você tem Bitcoin ou Ethereum parado numa carteira ou mesmo na exchange?
- Quer rentabilizar (em dólar ou criptomoeda) seus Bitcoins ou Ethereum?
- Quer conhecer as melhores estratégias para investir na Binance e Deribit?
- Tem receio de fazer trading e perder dinheiro?
- Quer aprender a fazer a gestão de risco dos seus investimentos?
- Se respondeu sim a alguma dessas questões, então podemos te ajudar.

Criamos a Serious Money para facilitar o acesso às estratégias que usamos em nossos investimentos, pois são estratégias lucrativas que, infelizmente, muita gente desconhece.

Por isso fazemos questão de oferecer essas estratégias diferenciadas, por meios acessíveis, para que mais pessoas como você possam ter acesso e obter resultados ainda melhores no investimento em criptomoedas.

Deixando claro que não operamos com seu dinheiro, ensinamos a operá-lo com estratégias vencedoras para que não dependa de ninguém (ninguém mesmo!).

A Serious Money é um projeto educacional criado por Christian Guerreiro e Augusto Gonçalves, especialistas em tecnologia da informação com mais de 20 anos de experiência no mercado de tecnologia e investimentos, em especial derivativos (futuros e opções) com criptomoedas.

Entre em contato conosco pelas redes sociais e tire todas as suas dúvidas sobre como podemos te ajudar!

OAB/BA:34.183

Bender Nascimento Banca & Advogados Associados, foi inaugurado nos idos de 2011 pelo Advogado Dr. Helinz Bender dos Santos Nascimento. Especialista em Advocacia Criminal; atua também na área Empresarial, Civil e Tributário. Entusiasta e estudioso das criptomoedas, inovações disruptivas e das relações jurídicas delas decorrente.

Whatsapp: (75) 99178 – 1105
Instagram: @Bendernascimento
Endereço: Av. João Durval Carneiro, 3253. Caseb.
Feira de Santana - Bahia.

Bitcoin é como a eletricidade primitiva. Bruto, perigoso, parece muito volátil e difícil de usar. Com o tempo, vai começar a parecer mais seguro, fácil e normal. Como a eletricidade, ela inspirará e impulsionará novas indústrias inimagináveis. E um dia vamos nos perguntar como é que vivemos sem isso?

@ObiWanKenoBit

Quando um cientista distinto e experiente diz que algo é possível, é quase certeza que tem razão. Quando ele diz que algo é impossível, ele está muito provavelmente errado.
O único caminho para desvendar os limites do possível é aventurar-se um pouco além dele, adentrando o impossível.
Qualquer tecnologia suficientemente avançada é indistinguível da magia.
Leis de Clark

Quanto mais sábia é uma pessoa, mais aborrecimentos ela tem; e, quanto mais sabe, mais sofre.
Eclesiastes 1:18

Se a miséria dos pobres não é causada pelas leis da natureza, mas por nossas instituições, grande é nosso pecado.
Charles Darwin

O Bitcoin foi projetado para ser protegido da influência de líderes carismáticos.
Satoshi Nakamoto

Caveats (advertência)**:** Nem um único conteúdo nesta obra é recomendação de investimento nem aconselhamento legal, nenhuma performance passada garante performance futura. Os coautores têm posições significativas de seu patrimônio nas nuvens. Bitcoin não é investimento, mas sim um *hedge* (proteção). Não existe investimento em ambiente de juro real negativo.

Maximalistas[1] consideram que: *shitcoins* como doge, shiba, bch e eth são ataques de engenharia social contra o Bitcoin; que mais de 90% dos *ICOs* são *scams* descarados; e, que se *DeFi* (finanças descentralizadas) é o futuro[2], provavelmente não será *onchain* — e sim em 2ª camada como *RSK*[3], *Liquid*[4] ou *Lightning*[5].

Altcoins foram úteis como alternativas para aumentar privacidade e escalabilidade de transações. Porém, não são mais necessárias para isso, elas podem ser úteis como *testnets* e como camadas de redundância para eventual falha na *mainnet*, mas a maioria das pessoas que tentam enriquecer ou “aumentar bitcoins” com *altcoins* acaba perdendo.

Ter valores depositados em corretora é risco de perda total, com falha na custódia; e, fazer *KYC*, informando seu nome, *e-mail* e endereço é risco de vida, de se tornar alvo de crimes ou perseguições totalitárias.

SUMÁRIO

PREFÁCIO
Só vamos sobreviver por causa do Bitcoin

Bitcoin Red Pill é o primeiro livro sério escrito em português sobre o Bitcoin. Diferentemente dos outros, é um livro que tenta dizer não só que é o Bitcoin, mas sim o porquê do Bitcoin. Não explica o Bitcoin somente como uma ferramenta, ou seja, qual sua função e mecanismo, mas mostra o Bitcoin como nossa única possibilidade de renascimento moral, material e tecnológico.

Este livro que não quer convencer ninguém. Você discorda que estamos em uma guerra de extermínio e que Bitcoin é uma das únicas armas à disposição do cidadão comum? Ótimo, faça o que você achar melhor para você e para sua família, siga sua vida como bem entender. Renato Amoedo e Alan Schramm só escreveram este livro porque estavam cansados de explicar várias vezes as mesmas coisas e, por interesse próprio, decidiram economizar tempo para tentar salvar o máximo de pessoas aptas. Infelizmente poucas pessoas neste mundo estão aptas a serem salvas. Se você se dispôs a ler este livro, muito provavelmente está entre elas.

Bitcoin Red Pill foi um livro escrito na era da internet para o indivíduo soberano. Como um manual de instruções, traz conceitos, teses, autores e dados que orientam o leitor a ir correr atrás das informações. A *internet* foi uma invenção magnífica pois diminuiu imensamente o custo da informação, mas é fácil se sentir desnorteado em sua galáxia. Bitcoin Red Pill mostra vários caminhos que podem depois ser trilhados pelo leitor interessado, seja este caminho sobre os aspectos técnicos sobre o Bitcoin, sobre a Escola Austríaca ou sobre colapsos civilizacionais.

Bitcoin tem pouco mais de uma década de existência. Um aspecto curioso de sua história é a quantidade imensa de pessoas com conhecimentos extremamente avançados de criptografia e programação que entenderam o Bitcoin só como “mais uma ferramenta”.

O que não falta é argumento de autoridade para confirmar essa impressão. O próprio Satoshi Nakamoto no *white paper* diz de forma muito sóbria que o Bitcoin é um “sistema de dinheiro eletrônico ponto-a-ponto”. Parece ser só mais uma mera ferramenta, não é mesmo? Sempre muito lacônico em suas correspondências, Satoshi confessou em um e-mail ser

melhor com *código* do que com palavras. Ainda bem: o Bitcoin funciona, isso basta.

No Bitcoin Red Pill, os autores buscam dizer o que Satoshi não diz: que tipo de sociedade humana o Bitcoin encontrou quando surgiu neste planeta e quais serão suas consequências mais profundas. Este é o primeiro livro brasileiro a navegar por nessas águas e traz um diagnóstico com o qual eu concordo integralmente: o Bitcoin encontrou uma natureza humana extremamente falha e encontrou também uma sociedade, a brasileira, repleta de golpistas, inflacionistas, malandros, *shitcoins* e pirâmides financeiras.

A escassez digital criada por Satoshi encontrou também um Estado completamente falido moral e financeiramente, que gasta mais que arrecada e joga a conta nas costas do povo por meio do roubo institucionalizado dos impostos e da inflação. O livro explica com detalhes as distorções de uma economia que gira com base em juros negativos e como funciona o Bitcoin, moeda forte e inconfiscável, num mundo de moedas estatais fracas e confiscáveis.

"Lembre-se de que a única coisa que ofereço é a verdade, nada mais", diz Morpheus. A pílula vermelha é a pílula mais difícil de engolir pois nos traz verdades que temos medo de admitir.

Renato Amoedo e Alan Schramm, além de trazerem relatos saborosos da história do Bitcoin no Brasil e de explicarem para o público leigo o funcionamento desta tecnologia e do mercado, foram corajosos o suficiente para oferecer este remédio amargo ao povo brasileiro.

Nesta segunda edição, lançada há menos de um ano da primeira, já vemos atualizações importantes devido à pandemia do vírus Sars-Cov-2. Os estragos desta pandemia criada em laboratório e da resposta ditatorial dos governos que fingem combatê-lo ainda não foram bem compreendidos amplamente. O que se sabe até agora não pegou o leitor da primeira edição Bitcoin Red Pill de surpresa: impressão massiva de dinheiro como nunca antes e propostas de controles de capitais ainda mais opressores por meio das assim chamadas moedas virtuais dos bancos centrais. A primeira edição saiu em setembro de 2020. Em julho de 2021 podemos dizer que as tendências apontadas pelo livro apenas se tornaram exponenciais.

Não há escapatória. Como dizem por aí, você pode não estar interessado na guerra, mas a guerra está interessada em você. Cada gráfico e cada linha

do livro é como um tapa na cara para acordar o brasileiro de um sono mortífero. Vai doer, mas valerá a pena.

— Guilherme Bandeira pesquisa e escreve sobre Bitcoin e sua regulação jurídica no Brasil. Foi tradutor do livro “O Padrão Bitcoin” para o português brasileiro e tem uma *newsletter* sobre o assunto https://guilhermebandeira.substack.com/publish

PRÓLOGO

Se quiser ir direto ao assunto, pule o prólogo - um roteiro com justificativas e análise contextual.

Certamente, o texto a seguir tem imprecisões, generalizações e erros, por isso não confie, verifique. Cada informação relevante tem referências em notas de rodapé ou no glossário. Temas mais complexos[6] vão ser objeto de volume posterior, *Bitcoin Black Pill - dinheiro, justiça e governo privados*.

Essa obra se dirige a facilitar a educação de pessoas dispostas a ser livres pela aquisição de fontes e conceitos para que viabilizem libertação pessoal e intelectual. “O início da sabedoria é chamar as coisas pelos seus devidos nomes”[7] – por isso se diz que “imposto é roubo”[8].

O livro foi escrito para economizar o tempo dos autores, que têm que explicar repetidamente a falsidade de diversos mitos. O Bitcoin (BTC). A cultura de criptografia e segurança digital é um bote salva-vidas para a liberdade e prosperidade de diversas famílias e uma das habilidades fundamentais para sobreviver financeiramente. Esse texto é um presente a quem quiser entender os motivos pelos quais:

1) Nos últimos 10 anos, não existiu nenhum produto financeiro de renda fixa (perda fixa) ou variável (perda variável, como as bolsas bolivarianas) com qualquer expectativa média de ganho real no *legacy*[9] (economia formal) – o que fica óbvio até mesmo pelo CDI e B3 (bolsa bolivariana do Brasil) perderem até do ouro guardado no colchão, sistematicamente, em ambiente de juros negativos e senhoriagem acelerada. Poupar em bitcoin é assumir alto risco, com alto potencial de ganho. Poupar em perda fixa ou perda variável é certeza de perda no longo prazo.

2) A maioria dos *traders* são viciados em apostas e as corretoras funcionam como cassinos. Não há como “viver de *trade*” sistematicamente – exceto se você tiver vantagem competitiva sobre os demais atores do mercado, seja na velocidade das execuções, vantagem na difusão ou acesso a dados ou notícias; ou vantagem na capacidade de manipular preço, o que não é o caso de ninguém que emprega dinheiro e tempo em cursos de *trade* vendidos no *YouTube*. A Literatura científica e lógica demonstra que, no longo prazo, mais de 95% das pessoas[10] se dão melhor empregando o tempo em seu trabalho (ou até mendigando), fazendo preço médio[11] e

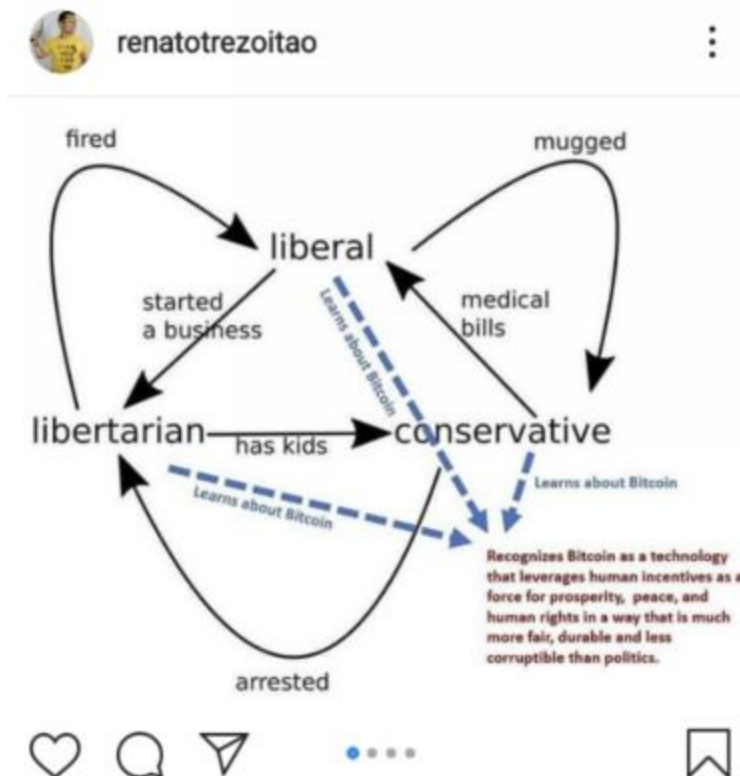
corrigindo a diversificação da carteira para manter proporção pré-determinada entre ativos, com rebalanceamento anual ou semestral. Só quem lucra sistematicamente nessa indústria são vendedores de cursos e relatórios e as corretoras, o resto é “catar moedas na linha do trem”[12].

3) Qualquer promessa de ganho sem esforço ou risco, como em “remuneração garantida acima do mercado”, é mentira: ou não há remuneração sistemática ou não é garantida[13]. As vítimas muitas vezes se enganam com o mantra “está pagando”. Ora, todos os esquemas *Ponzi* pagam enquanto entrarem mais recursos do que saírem. Não existe possibilidade de pessoas cumprirem perpetuamente rendimentos “garantidos” para fazer *trade* (que é realmente “ganhar de colher para perder de balde”) ou arbitragem (pior ainda, já que há deseconomia de escala em *slippage*[14]). Se você mandar bitcoins para um desconhecido, provavelmente não vai receber nada de volta – muito menos em dobro, como prometido nos golpes de *giveaway* (detalhados no capítulo II) com impersonificação de Elon Musk, Vitalik, Saylor e outras personalidades, como oferecido nesta live fake no Youtube.

4) Políticos, por mais bem-intencionados que sejam, não podem evitar o colapso e o totalitarismo por meios institucionais – como demonstrado por Olson, Hayek e Hoppe. Assim como os *déficits* sistemáticos e exponenciais dos Estados Sociais terminam, inevitavelmente, com a destruição de suas

moedas e de todos os ativos sob o alcance dos seus governos. "*Play stupid games, win stupid prizes.*"

5) Você só é dono dos bitcoins em endereços de que tem controle exclusivo das chaves privadas. Propriedade é um conceito absoluto. Se você tem saldo bancário (ou de ações ou até escritura de imóvel) e um burocrata pode revogar sua titularidade ou destruir seu valor com tributos (ou até regulações ambientais ou de zoneamento), então isso não é sua propriedade em seu conceito original, é outra categoria de direito. Ter saldo de bitcoins em corretora não é ter bitcoins (BTC). Assim como ter saldo de reais (moeda fiduciária) em empresa ou banco não é ter reais (é ter créditos que podem ser podres). Qualquer um pode criar endereços de Bitcoin em qualquer dispositivo, mesmo sem acesso à Internet. Qualquer um pode minerar, transacionar ou manter saldos em bitcoin sem autorização ou identificação. Ninguém controla o Bitcoin, nenhuma empresa, nem governo. O sistema não tem responsável nem chefe, não é possível impor sobre ele lei nacional ou decisão judicial, não há sequer quem citar em processos. Apenas empresas ou pessoas que operem com Bitcoin formalmente podem sofrer disciplina legal ou jurisdicional. "*Not your keys, not your coins*".

6) Os sinais de colapso civilizacional (dominância de valores femininos, *welfare*, diluição do valor da moeda, queda de fecundidade e de poupança, desestruturação de famílias etc.) são inevitáveis e cíclicos[15] (demonstrados por diversas teorias de ciclos intergeracionais, como a de Strauss-Howe ou de Sir John Glubb); e, em vez de se aborrecer com eles, é melhor aproveitar a crise como oportunidade e aceitar que Satoshi Nakamoto é John Galt[16].

7) O Bitcoin, se sobreviver por mais uma década, deve mudar o mundo mais do que a Internet já mudou – inviabilizando controles de capitais, expropriações e tributos involuntários, explodindo a erosão tributária, criando e destruindo mercados, e mudando brutalmente a hierarquia de valores. Quando o bitcoin desmonetizar ativos eles se tornam mais baratos: no caso do ouro, suas joias auríferas poderão ter mais peso pela metade do preço; com imóveis, você vai poder morar em um lugar muito melhor pela metade do custo; nos títulos e as ações, famílias vão voltar a ser remuneradas por poupança e poder viver de dividendos e juros reais. Já aconteceram e vão continuar a acontecer escândalos de manipulação de preço, ataques de spam, hacks em empresas, scams, proibições, ameaças de flippening com queda da dominância[17], criminalizações e restrições regulatórias e fraudes, mas "honey badger[18] don't care" (se o sistema continua rodando, o Bitcoin não se importa).

8) Moeda não é dinheiro. Em termos históricos, todas as moedas fiduciárias (*fiats*) emitidas por governos viraram pó ou tiveram a maior parte de seu valor perdido em termos reais (historicamente, em relação ao ouro). Assim como as coisas mais baratas da vida são pagas em moeda, as

demais são pagas com valores como sua liberdade, paz, saúde, amor, honra ou tempo de vida.

9) O maior investimento que se pode fazer é em educação real, que é, cada vez mais, oposta à instrução formal[19]. A verdade pode ser afirmada por critérios empíricos (como fatos históricos ou da realidade), ou por critérios lógicos (como a ética argumentativa *hoppeana*[20]), nunca por autoridade ou convenções[21] (como Direito Positivo[22]).

Red Pill vs Blue Pill

10) Os governos policialescos e totalitários travam uma guerra de extermínio contra a liberdade. Nessa guerra, as suas principais (embora não únicas) armas (para defender sua liberdade, patrimônio e modo de vida) são criptografia e descentralização. Se você não se prostrar à religião civil ponerológica, então, agora "o judeu é você" — seja hinduísta, *falun gong*, cristão[23] ou islâmico[24]. Todos os países serão infernos ou paraísos fiscais e regulatórios[25], não haverá meio termo, pode escolher:

Kim Jong Un warns that North Korea is running out of food as reports say a bunch of bananas now costs $45

Bill Bostock 11 hours ago

North Korean leader Kim Jong Un at a party meeting in Pyongyang, North Korea, in an undated photo released Wednesday by state media. KCNA via Reuters

ESTADOS UNIDOS MEJORA LA CALIFICACIÓN DE VIAJE PARA EL PAÍS

$0.25

Diario El Salvador

Loki llega hoy

ASAMBLEA APRUEBA LA LEY BITCOIN

La criptomoneda tendrá curso legal en el país. El BCR reafirma solidez del uso del dólar.

Países hermanos

LA FESFUT DEBE REGISTRARSE ANTE EL INDES ANTES DEL 30 DE SEPTIEMBRE

$245 MILLONES

DESTINADOS PARA CONSTRUIR EN LOS CHORROS EL VIADUCTO FRANCISCO MORAZÁN

ENCUESTA UTEC REVELA APOYO DEL 81.96 % AL REGRESO DE LAS CLASES SEMIPRESENCIALES

CON BOLETO A LA SEGUNDA RONDA 3-0

11) É relevante conhecer as dez operações básicas no ecossistema, seus prós, contras e quando e a quem são indicadas (*trade; hold; lend/margin trade; loan/*colateralizado; *scam; ransomware; bounty;* arbitragens*;* mineração e empreendedorismo).

Se já dominou os conceitos e ideias acima mencionados, não precisa continuar lendo.

Não se deve emitir opiniões públicas sobre assuntos técnicos para os quais não se tenha dedicado algumas milhares de horas em estudo ou experiência. Descobrimos o que realmente era o Bitcoin no início de 2015 e, após isso, temos dedicado a maior parte do tempo a compreender e interagir com o ecossistema.

Aprendendo com os erros dos outros, evita-se o prejuízo. Da mesma maneira que dependemos de tutores no início da nossa jornada, temos o dever de facilitar o caminho dos que vêm depois, fazendo nossa parte como a "*pleb"* do neofeudalismo de Max Keiser, que logo será a nova nobreza natural, após cumprir a missão como "*cyber hornets"*[26].

Mises Capital vs Samy Dana[27]

Michael Saylor
@michael_saylor
#Bitcoin is a swarm of cyber hornets serving the goddess of wisdom, feeding on the fire of truth, exponentially growing ever smarter, faster, and stronger behind a wall of encrypted energy.
Traduzir Tweet
3:51 PM · 18 de set de 2020 · Twitter Web App
4.009 Retweets 725 Tweets com comentário 20 mil Curtidas
Eiran Simis @eiransi... · 09 dez 18
A quantidade de Bitcoin é conhecida, já a de ouro ninguém sabe ao certo. Mas na dúvida é bom ter os dois.
1 8
Henrique Bredda
@hbredda
Em resposta a @eiransimis @Vinicius1_Bsb e @JamesGRickards
Bitcoin?! Pra q complicar? Sai dessa.
21:46 · 09 dez 18 · Twitter for Android

É uma honra viver esse momento da história, em que dezenas de paralelos dos colapsos civilizacionais se repetem, tais como: queda de fecundidade, efeminação[28] e infantilização de pautas públicas, diluição da moeda, *welfare* deficitário, desestruturação de famílias, corrupção e ampla captura administrativa. O Bitcoin é uma das tecnologias para servir de "bote salva-vidas" para quem perceber a realidade, por isso se diz que "cada um compra (e vende) o bitcoin no preço que merece" ou "quem não comprar bitcoins sorrindo, vai comprar satoshis chorando".

Se você é capaz de ler com boa velocidade e aproveitamento em inglês, então, para aprofundar, leia *The Internet of Money 1,2 e 3*, do Andreas Antonopoulos, e, se for programador, o *Mastering Bitcoin*, do mesmo autor, ou *Programming Bitcoin: Learn How to Program Bitcoin from Scratch*, de Jimmy Song. Um manual passo a passo é o *21 Lessons: What I've Learned from Falling Down the Bitcoin Rabbit Hole.*

O *opus magnum* em português é *O Padrão Bitcoin*, de Saifedean Ammous.

Esses livros são superiores, em muitos aspectos, a qualquer outra coisa e são facilmente encontrados, gratuitamente, na Internet. A leitura do verbete *Bitcoin*[29] na Wikipédia (em PT e EN) ou Bitcoin WiKi[30] (EN) também são excelentes como primeiros passos.

Sobre as implicações políticas e sociais do Bitcoin, recomenda-se *Bitcoin Revolution: Ending Tyranny For Fun & Profit*[31].

Se você não sabe quem é Menger, Bawerk, Mises, Hayek, Rothbard, Hoppe e os Friedmans (os três), é altamente recomendado que busque suas obras seminais – igualmente disponíveis em português em diversos PDFs gratuitos na Internet nos sites dos Institutos Mises Brasil[32] e Rothbard Brasil[33].

Não precisa ser libertário para ser *bitcoiner*. Diversas figuras no país e no exterior (como o próprio Andreas Antonopoulos) têm tendências "esquerdopatas" claras. Porém, se não compreender os autores acima mencionados, não entenderá os conceitos de lastro, moeda fiduciária (*fiat*), dinheiro, senhoriagem, reserva fracionária, ciclos econômicos e as reais consequências da guerra ao dinheiro e dos juros negativos.

Sem compreender a Escola Austríaca, não entenderá em sua totalidade conceitos como: captura administrativa, Lei de Gresham, Lei de Wagner, Lei de Michels, Curva de Laffer, Efeito Cantillon; fatores estruturais deflacionários (demografia/envelhecimento, desalavancagem bancária, disrupção tecnológica); a insustentabilidade dos níveis de endividamento máximos, públicos e privados; a velocidade da moeda; e, a diferença entre inflação, base e agregados monetários[34] e os índices de preços.

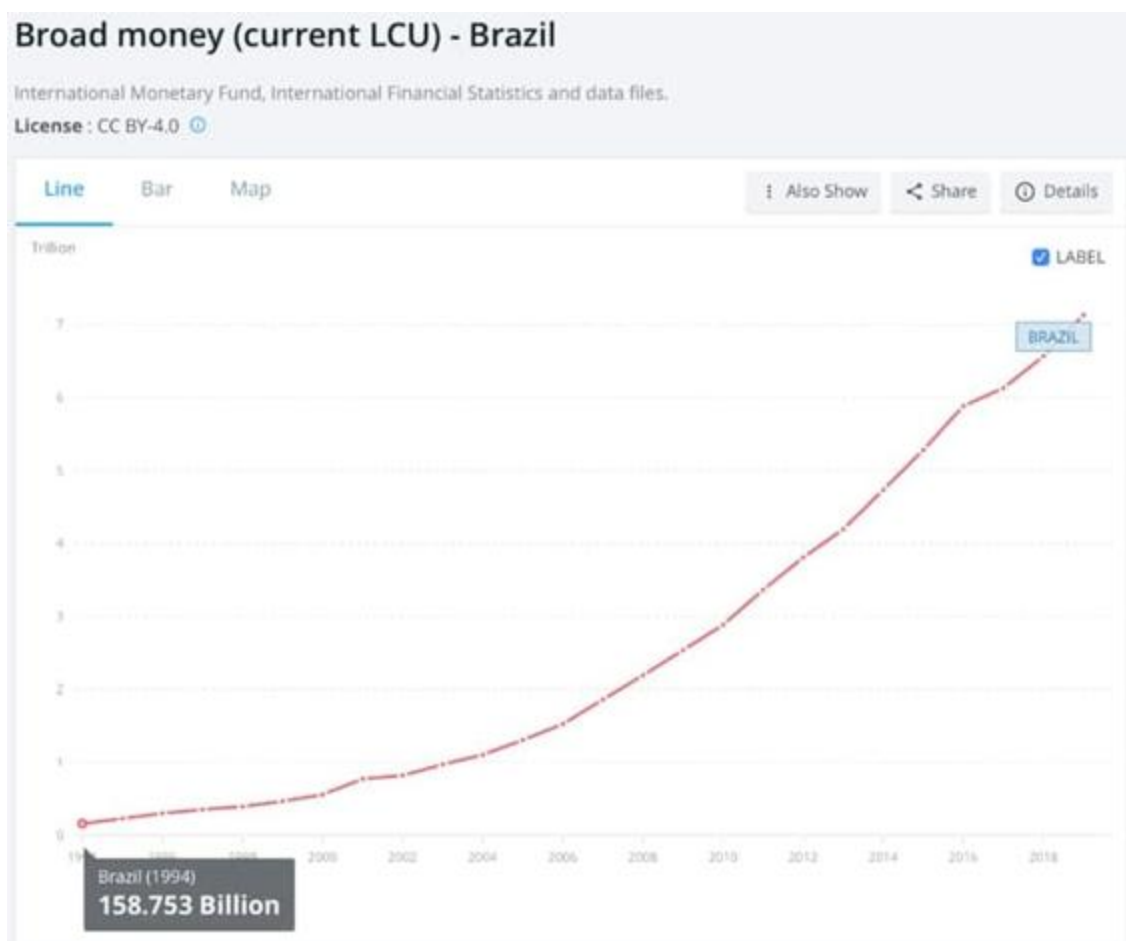
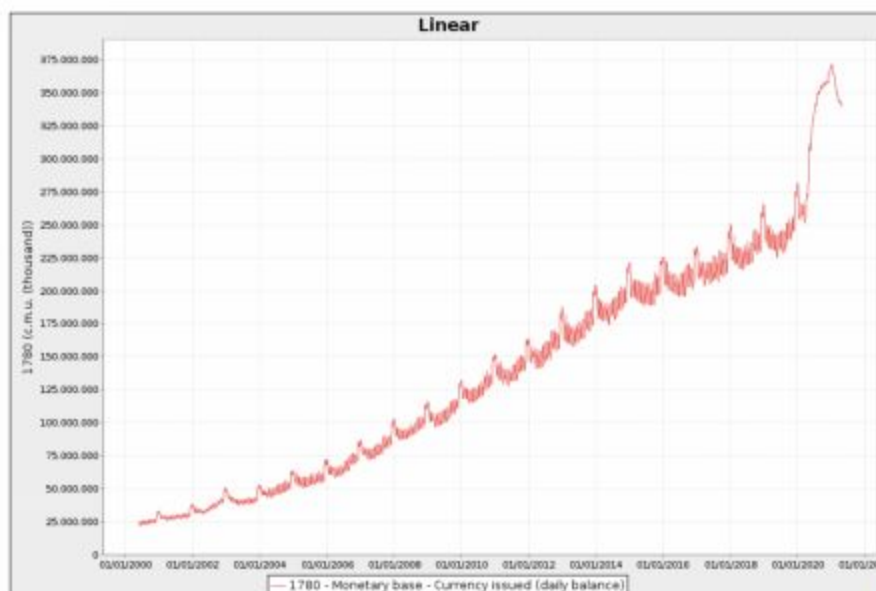
O entendimento da realidade, lógica ou empírica, é a educação real.

É devido a esses fatores deflacionários que o governo conseguiu aumentar os agregados monetários (base monetária e dívida pública) por mais de 10 anos em mais de 10% ao ano (em média) e ainda manter alegações de que remunerações patéticas de um dígito são “juro real

positivo”. A vovó *nocoiner* recebe 90% do CDI (menos de 5%aa), tem mais de 15% de perda real (devido a inflação) e ainda tem que pagar imposto de renda.

Quando você compreende que o mundo – e o Brasil – vivem em um ambiente de juro real negativo (descontado o aumento da base monetária e o risco), entende que nenhum produto financeiro convencional pode ser considerado investimento. Aí, sim, é possível entender por que produtos como ouro[35] (que sequer pode ser considerado investimento) ganharam da inflação oficial e até mesmo do aumento do salário mínimo desde o início do Plano Real.

Hipoteticamente, se a economia no país crescesse, em média, 1% ao ano na década e o total de meio circulante aumentasse em mais de 20% a.a., o governo enriqueceria, diretamente, em 19% ao ano devido à nova moeda criada; e, indiretamente, através do aumento de impostos decorrente.

Como é demonstrado nos gráficos, a realidade é pior que isso[36]:

Segundo o Banco Central do Brasil[37]: "A base monetária alcançou R$427,8 bilhões em outubro, aumento de 4,7% no mês e de 46,3% em doze meses” (gráfico abaixo, também do BCB, não cobre período recente)[38]. Ora, se o PIB caiu e o número de reais aumentou em mais de 46% em 2020, quanto foi a perda de quem poupou em reais, mesmo que remunerado pela SELIC (abaixo de 3% em 2020)?

No resto do mundo, a situação não é muito melhor, os agregados monetários globais (moedas de todos governos) cresceram em um ano (até meados de 2021) mais de 32% do PIB global e os mercados comemoram um crescimento estimado em 6% a.a. (medido nessas moedas diluídas em 32%, resulta em perda real de 26%).

Há três formas principais de governos se financiarem: a) tributos (limitados pela curva de Laffer); b) emissão de moeda (limitada a destruição de valor do meio circulante, como na Venezuela e no Zimbábue); e, c) emissão de dívida (limitada a disposição de credores a emprestar). As três fontes estão próximas dos limites.

As consequências de aumentar a carga tributária são: 1) o aumento dos custos de produtos e serviços e a destruição de riqueza devido às transações que deixam de ser realizadas por essa subida de preços (perda do bem-estar social); 2) enriquecimento de "aspones" e empobrecimento de produtores e consumidores; e, 3) decomposição de instituições, com ampliação das vantagens de comportamentos oportunistas.

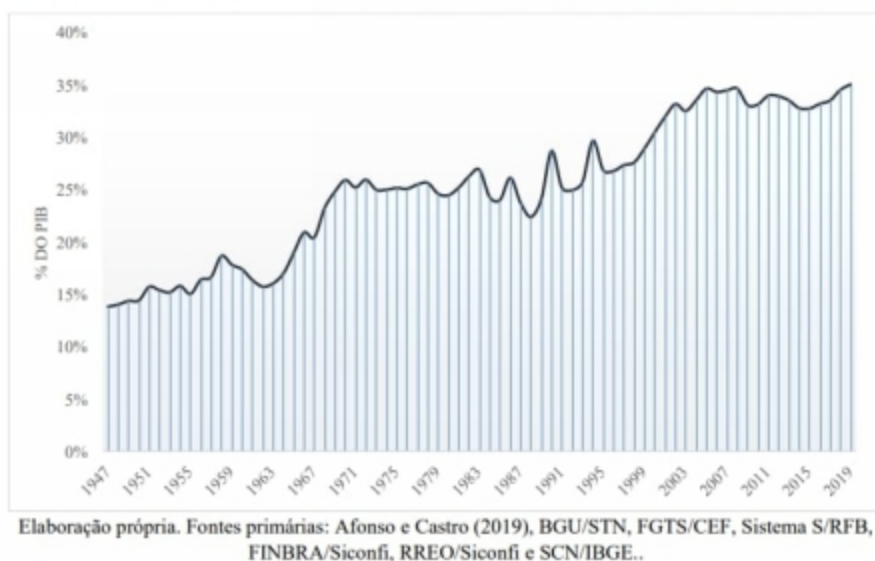
Se um banco central emite mais moeda, ele dilui o valor daquelas já existentes (inclusive o valor de sua própria dívida em moeda soberana), e destrói a riqueza de quem poupou em *fiat*, traindo e empobrecendo quem confiou nele.

Quando o governo emite dívida, ele retira investimentos que iriam para atividades produtivas, e destrói todos os empreendimentos com expectativa de retorno corrigida pelo risco, inferior à remuneração de seus títulos.

Também no gasto dos recursos arrecadados, o Estado destrói riqueza, uma vez que seus gastos não respeitam critérios de mercado e competem com os entes que realmente geram riqueza, e eleva para esses o custo dos bens e serviços que venham a adquirir. O "monopólio da violência" é uma máquina de produzir corrupção, miséria e terror.

Você realmente acha que há alguma chance de as curvas de carga tributária e *déficit* serem invertidas? Como proteger sua família disso?

Gráfico 1 - Evolução Histórica da Carga Tributária Bruta no Brasil- 1947/2019

Elaboração própria. Fontes primárias: Afonso e Castro (2019), BGU/STN, FGTS/CEF, Sistema S/RFB, FINBRA/Siconfi, RREO/Siconfi e SCN/IBGE..

Com dados mais atualizados, seria ainda mais brutal a demonstração dos *déficits* públicos, carga tributária, aumento dos agregados e endividamentos estruturais.

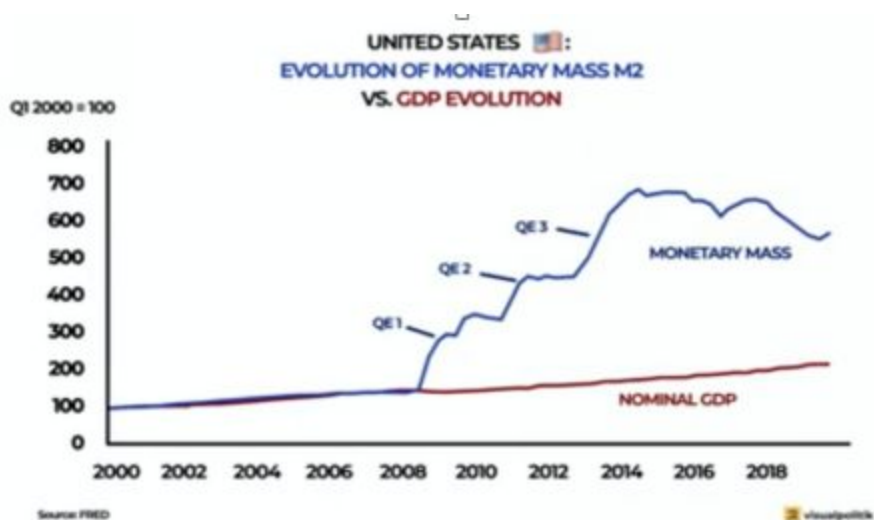
Se você investiu em qualquer coisa que não rendeu líquido e descontado de risco mais de 46,3% em 2020 em reais, perdeu riqueza, era melhor ter estocado bem não perecível ou comprado galinhas. A única medida objetiva de inflação é o aumento da base monetária, que foi superior a 20% a.a. em Real (R$ ou BRL) nos últimos anos (somando reais criados por meio das reservas fracionárias dos bancos e pelo governo).

Esses efeitos não são percebidos por muitos, devido aos fatores estruturais de redução de preços, porém, suas consequências em longo prazo são inexoráveis – uma vez que os fatores deflacionários não são perpétuos. Quem não perceber, vai sofrer. O Brasil envelhece 6,5x mais

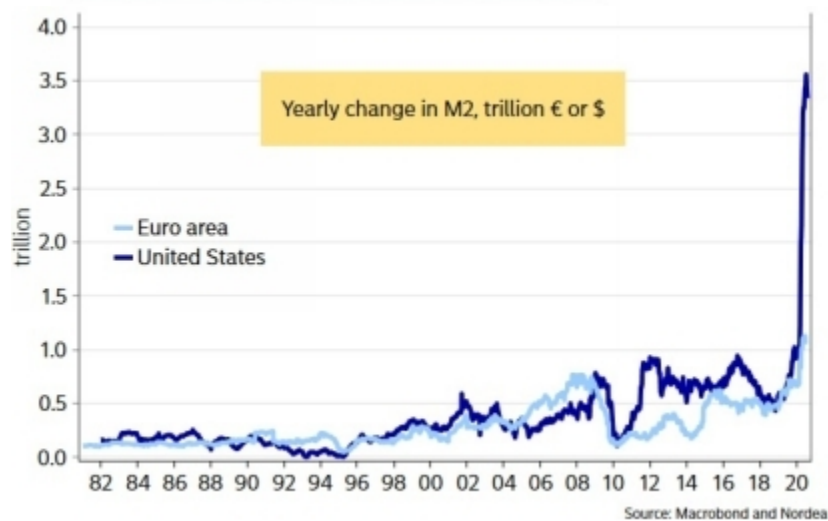
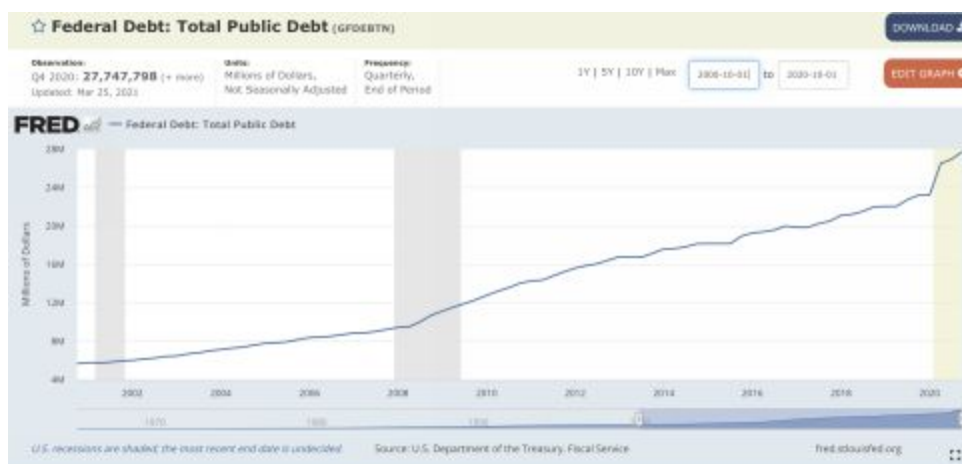
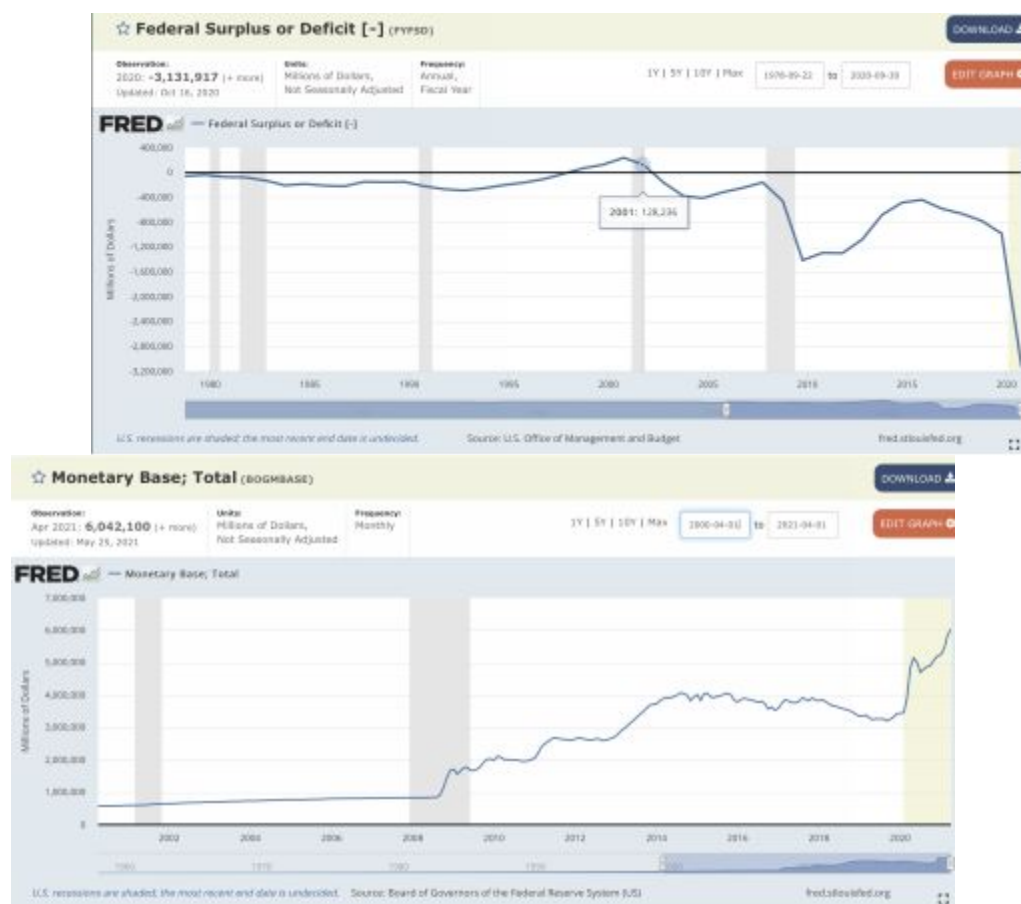
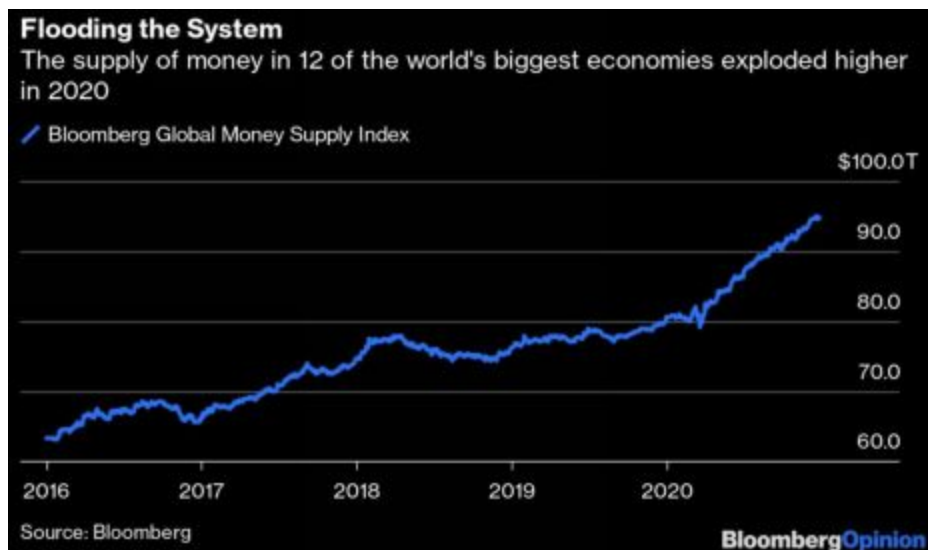
rápido que os Estados Unidos e o dividendo demográfico já foi desperdiçado.

O imposto inflacionário (*hidden tax* de Friedman) não apenas dilui o valor dos reais (moeda fiduciária), como aumenta o pagamento de impostos de renda, via aumento do valor nominal dos bens e dos salários[39]. Ora, se um bem (seja casa, carro, ação ou barra de ouro) que custava 100 reais é vendido 30 anos depois por 100 mil reais, formalmente, 99,9% do seu valor de venda seria "lucro" para fins tributários, mesmo que seu valor real 30 anos depois fosse inferior ao seu valor real original. Exemplo claro é o grama de ouro: sua cotação em julho de 1994 foi R$ 11,45; se vendido em maio de 2020, quando a cotação chegou a R$ 321,35, formalmente, 310 reais seriam "lucro" e tributáveis, mesmo que esses 310 comprassem menos bens em 2020 do que 11,45 compravam em 1994.

Ou seja, o imposto inflacionário aumenta a arrecadação ao inflar nominalmente a renda; amplia a capacidade do Estado de se endividar ao reduzir o valor real de sua dívida; dilui o valor dos detentores de moeda e títulos de dívida, empobrecendo quem confiou no governo; e subtrai das famílias os benefícios deflacionários da tecnologia. Por isso, a inflação deve ser medida por aumento da base monetária e não por índices de preços, como IPCA, no Brasil, ou CPI, nos EUA, (usualmente manipulados).

Grandes mentes discutem ideias, mentes medianas discutem
eventos, e as mentes pequenas discutem pessoas.

"A study by Hirschman Capital shows that out of 51 cases of govt debt breaking above 130% of GDP since 1800, 50 governments have defaulted. The only exception, so far, is Japan. We mention this because the IMF expects US Debt to hit 141% by the end of 2020."

Felix Zulauf

11:03 · 23 Aug 20 · Twitter for iPhone

Embora no *whitepaper*[40] original Satoshi não tenha feito qualquer consideração explícita sobre política ou economia, a mensagem incluída no Bloco Gênese[41] do Bitcoin e as postagens em fóruns[42] do seu criador, Satoshi Nakamoto, deixam claro que o Bitcoin só se tornou necessário devido aos abusos dos governos em emitir moeda desenfreadamente (até agora o número de reais criados pelo governo aumentou mais de 45x nominalmente e mais que triplicou, em relação ao PIB, desde 1994) e em manter níveis exponenciais de *déficit*, vide o governo norte americano, que gasta mais do que arrecada desde 2001[43]:

O resultado disso é a explosão na base monetária do dólar, em mais de 10x, e da dívida pública, em mais de 5x, nos últimos 20 anos:

Moeda puramente fiduciária (*fiat*) é a que não é conversível e só é aceita por imposição legal, denominada “curso forçado”[44], como o real ou o euro. O poder de emissão ilimitado cria estímulos perversos para que *déficit* e endividamento exponenciais sejam uma constante e atinjam níveis sem precedentes. Há 10x mais riqueza em *fiat* que em ouro[45]:

As políticas de guerra ao dinheiro (restrição de uso e propriedade de moeda alodial[46]) e os juros negativos permitem ampliar ainda mais o endividamento público e o totalitarismo financeiro.

Exemplos dessas limitações ao uso e à propriedade da moeda física, ouro e outras formas de moeda alodial são, desde 2015[47], as restrições de uso de moeda para transações privadas na Itália, na França e na Espanha (coroadas com a retirada de circulação das cédulas de 500 euros[48]); e a propriedade limitada sobre ouro na Alemanha e na Índia, e proibida nos Estados Unidos de 1934 a 1975[49].

O resultado do juro real negativo, além da elevação artificial dos valores dos ativos, foi a desigualdade social sem precedentes. O juro mundialmente apresentava tendência de queda desde 1981, mas o ápice do processo foi demonstrado na última década, em que até ouro[50] no colchão superou métricas como o índice Bovespa ou o CDI (ou seja, qualquer investimento bancário sem riscos extremos) – o que tende a se agravar com a normalização dos juros e destruição de valor dos ativos convencionais (*legacy system*).

Como demonstrado nas fórmulas do valor presente líquido e do *CAPM*[51] (considerando riscos de mercado e idiossincráticos), os ativos que têm fluxos de caixa independentes de taxas de juros (como ações, pontos comerciais e imóveis para aluguel) são usualmente avaliados pelas expectativas médias de fluxos descontadas das taxas de juro. Ou seja, considerando os riscos na expectativa média de retorno, um ativo qualquer que gere renda teria a sua avaliação equivalente ao quanto de moeda no sistema bancário pagaria no juro de mercado; quanto menor a taxa de juro, maiores ficam as avaliações dos ativos, *Ceteris Paribus* (considerando demais fatores constantes).

Nesta simplificação, se uma casa gera aluguel de R$ 1.000 por mês independente de taxa de juro e a taxa é de 1% ao mês (12,68% ao ano), a casa valeria R$ 100.000, pois 1.000 é 1% de 100.000. Se a taxa de juro cai para 0.1% ao mês, agora ela gera fluxo equivalente a R$ 1.000.000, pois 1.000 é 0.1% de 1 milhão; e, se o juro cai para 0.1% a.a, são necessários mais de R$ 12.000.000 (doze milhões) em investimentos para equivaler a seu aluguel.

Imagine agora o tamanho da distorção (e de como estão inflados os preços de imóveis e ações) quando os juros reais (descontados da inflação) são negativos e o quanto os ativos podem se desvalorizar quando os juros voltarem ao normal. Este também é o motivo de haver enorme potencial de desvalorização dos ativos com a normalização de juros.

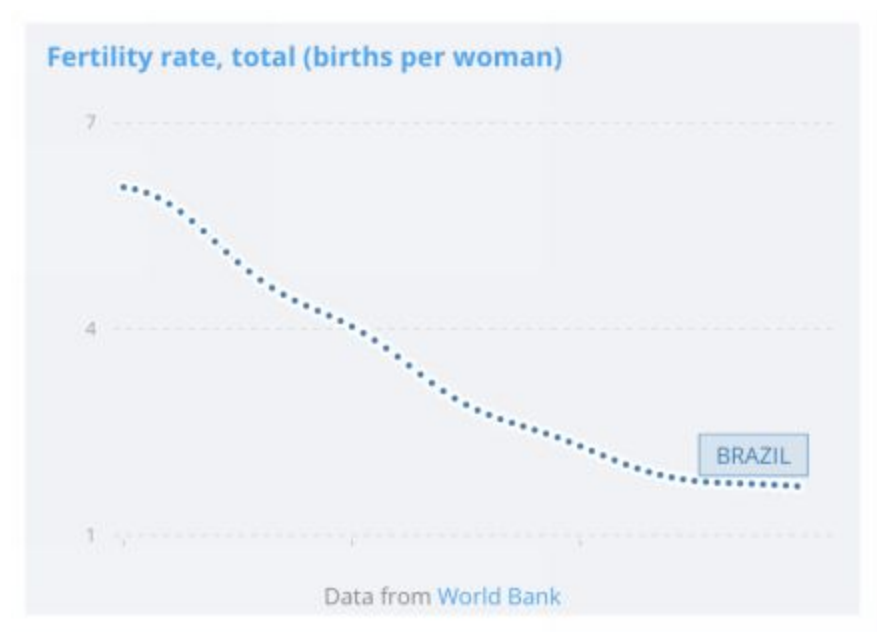
Além da captura administrativa[52], esse tabelamento imoral de preço foi a principal causa do aumento das desigualdades sociais no mundo, nas últimas décadas. Primeiro, multiplicando em ordens de grandeza a avaliação dos ativos dos “ricos” (às vezes apenas sua residência, que em muitos centros urbanos multiplicou centenas de vezes de valor nominal em gerações); e, segundo, desestimulando a poupança (facilitando endividamento subsidiado, com hipotecas, como bem descrito no filme *The Big Short*). Por isso, os bilionários multiplicaram suas fortunas, enquanto os micro e pequenos empresários foram obliterados no caos social[53] decorrente do vírus chinês, no que se denominou “recuperação em K” - *wall street* para cima, *main street* para baixo[54] (privilegiados, cantilionários para cima e empreendedor honesto das classes média ou baixa, destruído).

Além da destruição de valor derivada da normalização dos juros, outros dois fatores vão corroborar a perda de valor dos ativos convencionais (imóveis, ações e títulos): primeiro, a reação agressiva dos governos

(sistematicamente deficitários) em face das quedas na arrecadação (erosão tributária, elevação dos níveis de regulação e tributação); e, segundo, as mudanças tecnológicas, que tornam grande parte (se não a maioria) dos imóveis, ações e moedas obsoletos. Teletrabalho e comércio virtual reduzem a demanda por imóveis comerciais, como grande exemplo dessa tendência[55].

Assim, quem conta com investimentos em imóveis, ações ou títulos pode ter seu futuro comprometido como aqueles que contavam com aluguel de linhas telefônicas, placas de táxi ou dividendos da *Kodak*.

Quem conta com previdências privadas ou públicas não está em melhor situação. As previdências por capitalização são inviáveis em regime de juro real negativo (investimentos perdem sistematicamente valor, inclusive com taxas de administração) e as previdências por sistemas de caixa (repartição) são matematicamente inviáveis com taxas de fecundidade (e taxas de emprego e contribuição) insuficientes e decrescentes (fecundidade no Brasil cai desde 1950, já está abaixo de 1,7 e seria necessário estar acima de 2,2 para manter a população estável).

A população brasileira já envelhece exponencialmente desde 2018 e, com o fim do dividendo demográfico[56], tende a cair após 2030-2040[57], até que as motivações para ter famílias numerosas voltem a existir:

A infância mental[58] é denotada pelas decisões e reações emocionais em vez de racionais, pela efeminação da sociedade[59] e pela incapacidade de assumir responsabilidades básicas, atribuindo a outras pessoas ou instituições a obrigação de resolver seus problemas pessoais e a culpa pelas suas derrotas, como se observa nos eternos adolescentes que acreditam que "o Estado tem dever de dar educação e saúde gratuitas"; ou aqueles que, sem trabalhar, "estudam para concurso" ou fazem a terceira ou quarta graduação aos 30 (como Charlinho do Hermes e Renato, educacionistas); ou aqueles fracassados que culpam sombras pelo sua derrota – terceirização moral –, seja a sua cor, os judeus, o "capitalismo opressor" ou os seus pais. Quando alguém entende que "ninguém te deve nada", torna-se adulto mentalmente.

Se optar por tomar a *Matrix red pill* e ser livre, vai passar a ser responsável – vai ter que estudar, entender e assumir as consequências de seus atos. Liberdade absoluta é responsabilidade absoluta.

Ser livre não é sinônimo de fazer o que tiver vontade. Quanto mais autodisciplina e autocontrole, quanto mais entendimento, mais liberdade, mais poder e mais responsabilidade. Então, se está pronto para deixar a infância política, mental e financeira, pode continuar.

Já está mais que consolidado que a instrução formal hoje é oposta à educação real – como já demonstraram Taleb e Robert Kiyosaki no livro *Fake money, fake teachers and fake assets* (Ativos, moedas e professores de mentira). Bill Gates e Zuckerberg largaram os estudos para empreender, Amancio Ortega e Steve Jobs nunca foram alunos de qualquer faculdade e Thomas Edison largou a escola no segundo mês. Isso sem contar os exemplos de sucesso sem formação universitária no país, desde Luís Inácio e Alcolumbre até os bilionários Joesley e Wesley Batista – que sequer terminaram o colegial.

Testes oficiais, como ENEM e ENADE, indicam que a maioria dos universitários no país são analfabetos em algum grau.

No passado, o consenso era o pensamento mítico e mágico e abordagens concretas e objetivas eram minoritárias: alquimia era dominante e química estudo marginal; astrologia foi dominante por séculos e astronomia era marginal.

Hoje, com a academia profundamente infiltrada e subvertida[60], disciplinas inteiras continuam dominadas por pseudociência, misticismo e ideologia pura, como a Nutrição baseada em Ancel Keys[61], a Economia baseada em marxistas e keynesianos, ou o Direito baseado em Direito Positivo – refutado desde seu início – ou em ativismos ainda mais baixos (intelectual e moralmente).

Políticos têm interesse que as crianças do povo sejam educadas para serem independentes, ricas e inteligentes, ou dependentes, pobres e imbecilizadas?

Quando alguém compreende a resposta desta pergunta, entende que o governo/socialismo/comunismo não é incompetente. Ao contrário, o governo é ALTAMENTE eficiente em aumentar o poder do Estado e a riqueza dos governantes – incluindo aí todo estamento burocrático: os eleitos, o *deep state*, os “aspones” concursados e, especialmente, os “amigos do rei” ou “consórcio”[62], como prefere Olavo de Carvalho em *Os EUA e a Nova Ordem Mundial*, ao se referir aos maiores beneficiários da “captura administrativa”, degeneração derivada do aumento do Estado além de suas funções próprias de jurisdição e defesa.

Olavo de Carvalho[63] atingiu seu nível de popularidade e influência exatamente por despertar na população o entendimento de que: 1) o coletivismo é expressão do mal absoluto (em termos de direitos naturais ou até espirituais) – trazendo a público fontes como Eric Voegelin[64], Lyle Rossiter (Mentalidade Esquerdista), Lobaczewski (Ponerologia Política) e Solzhenitsyn (Arquipélago Gulag); 2) o Estado tende a aumentar seu poder exponencialmente, como descrito no *Jardim das Aflições*, apenas com argumentos retóricos e históricos, como os de Jouvenel (*O Poder: história natural do seu crescimento*); e 3) o meio de aumentar os poderes do Estado de maneira exponencial é a engenharia social, planejada e insidiosa, destruindo a inteligência pela instrução formal controlada por burocratas, desestruturando as famílias com leis feministas e estímulo à promiscuidade, infiltrando e subvertendo instituições sociais (incluindo aí a moeda),

infantilizando eleitores e efeminando homens (corrupção da inteligência) [65].

Os problemas do Professor Olavo[66] com os pagamentos do seu curso são excelentes exemplos da urgência da educação em relação a criptomoedas. Se o curso fosse pago em bitcoin, ou outra cripto pseudo-anônima, nem que fosse *stable dollar*, problemas com o *Paypal*, PagSeguro e *IRS (Internal Revenue Service)* ou RFB (Receita Federal do Brasil) seriam evitados – e a identidade dos alunos preservada, em vez de exposta a governos e corporações militantes para expurgos presentes e futuros.

Assim como a educação pública não visa educar, a imprensa progressista não tem como objetivo informar nem convencer. Ela tem como objetivo intimidar, amedrontar e dessensibilizar as vítimas (subversão e contrainteligência). **A maior parte das concessões públicas visa abertamente à desinformação, à inversão de valores morais e às “*fake news*”, como popularizado por Trump.**

A infância política é identificada pelo cultivo da “Arrogância fatal”[67], crença irracional de que a sociedade pode ser planejada e regulada positivamente por uma autoridade central sem qualquer *“skin in the game”[68]*, devidamente refutada por Hayek, dentre outros, no *“O uso do conhecimento na sociedade".*

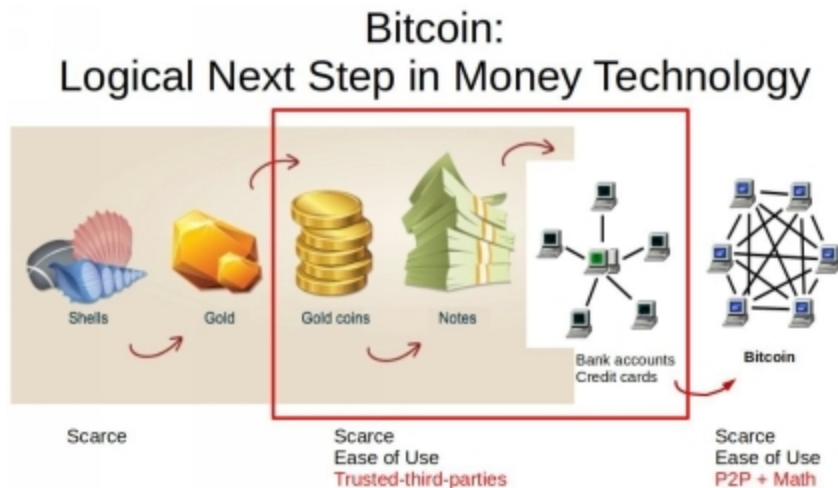
A infância financeira[69] advém da crença de que é possível constituir riqueza – ou mesmo manter padrão de vida – pagando metade de sua renda de tributos e usando a outra metade para pagar por aquilo que já pagou ao Estado para te prover. Essa condição de infância é usualmente evidente em quem usa moeda estatal exponencialmente diluída para acumular sua poupança na “perda fixa”; para quem confia em contribuições a sistemas de previdência insustentáveis; ou para os “arrojados” que confiam o futuro de suas famílias exclusivamente na compra de ações de empresas e fundos submetidos à soberania de Estados Sociais. Se quiser entender melhor que dinheiro é a forma de concentrar TEMPO e LIBERDADE, assista no *YouTube* a *Hidden secrets of money[70]*, com Mike Maloney.

Se o leitor tiver menos de 40 anos, provavelmente não vai receber nada significativo de aposentadoria, mesmo que seja servidor público. Caia na real: de onde acha que o governo brasileiro vai tirar dinheiro para pagar aposentadoria em 35 anos quando for o país mais velho das Américas? Sua poupança e sua eventual herança em 10 anos poderão não valer nada, como os ativos dos venezuelanos, que viraram pó. A solução está no

conhecimento. Se continuar a leitura, vai ser exposto a verdades que podem te libertar.

Por esses motivos, foi criada uma alternativa de reserva de valor superior ao ouro em certos critérios aristotélicos do DINHEIRO: o Bitcoin. Os atributos de moeda são fungibilidade (as unidades serem indistinguíveis umas das outras), divisibilidade, durabilidade, transportabilidade e, se além de moeda for dinheiro, deve ter o atributo da escassez (para servir de reserva de valor). O bitcoin é mais divisível, mais transportável, mais fungível; já é mais escasso em oferta marginal (inflação anual) que o ouro após maio de 2020; e até agora tem sido durável, embora nesse critério o *track record* do ouro imponha superioridade com milhares de anos e maior resiliência.

Pontas de flecha, contas (para fazer pulseiras e colares) e ferramentas de obsidiana (rocha magmática) foram demonetizadas pelo cobre. O cobre foi demonetizado pela prata. A prata, pelo ouro. O ouro, por *fiats*. Agora, *fiats* estão sendo demonetizadas pelo Bitcoin, a abstração suprema. Esse processo ocorreu no mundo em milênios — e no Brasil em poucos séculos com os indígenas, denotando ser orgânico[71].

Em todos os processos anteriores, os “amigos do rei” enriqueceram às custas dos poupadores. Agora, o varejo (a *pleb*, pequeno investidor) enriqueceu antes do *legacy* (instituições tradicionais, fundos, bancos e governos). Por isso, Bitcoin não é a oportunidade da geração, mas a oportunidade da história da humanidade.[72]

Há falha grave na argumentação de quem defende que a morte das moedas fiduciárias, o fim das empresas zumbis e a irrelevância de governos

são processos inevitáveis devido à queda dos custos de transação e aumento dos custos administrativos (como detalhado por Coase[73] e Calabresi/Melamed[74]). Quem prevê a inevitabilidade do futuro baseado em projeções de tendências econômicas são os marxistas e malthusianos – ambos erram completamente. Neste aspecto, há mais razão com o Paulo Kogos do que com Peter Turguniev.

A engenharia social da “fraudemia” deixa claro como populações podem aceitar a destruição de grande parte da economia privada e a revogação de liberdades com base em mera propaganda estatal ou atos abertamente ilegais.[75]

Há pessoas muito inteligentes que não entendem a urgência e utilidade do Bitcoin, simplesmente por viver em bolhas de crença na legalidade e legitimidade estatal. Se você acredita que o governo te deu educação, saúde e segurança – e que a moeda emitida por ele te protege de perdas – não haveria porque migrar para as nuvens. Classe média do primeiro mundo, aspones, marajás, empresários amigos do rei e os mais corrompidos moralmente vão ser os últimos a aceitar[76]. Por isso que se diz que o Bitcoin é um buraco negro que atrai primeiro aqueles elementos de maior massa e densidade, intelectual e moral[77].

Procedimentos de *lockdown*[78] (confinamento de gente inocente e saudável) sem qualquer fundamento empírico ou lógico (que destroem empresas, empregos e poupança) ou a obrigatoriedade de uso de máscaras de pano ineptas e insalubres[79], mesmo após resultados superiores (em instituições, economia e imunidade de manada) em países que não adotaram o *lockdown*, como Suécia e Uruguai, demonstram como a humanidade pode perder liberdades e riqueza rapidamente e sem motivo real, vez que a mortalidade da doença é de menos de 2% em septuagenários (*Diamond Princess*)[80] e de menos de 1:1200 em saudáveis (*USS Theodore Roosevelt*)[81], sem tratamentos específicos.

Trata-se de arrogância fatal prever o resultado de futuras interações de mercado entre bilhões de agentes. Como experiências de ditaduras totalitárias na China, Cuba e Coreia do Norte provam, governos podem, sim, interferir em custos de transação, e novas tecnologias podem reduzir brutalmente os custos administrativos e de controle social. Várias tecnologias superiores em diversos aspectos já foram rejeitadas no teste real de eficiência no mercado — ou por interferência regulatória.

Essa argumentação indica que a *web* 1.0 (sites estáticos e não interativos) foi capaz de tornar serviços postais obsoletos com os *e-mails*, locadoras de DVDs e venda de CDs igualmente eliminados por serviços de *download*; a *web* 2.0 (*sites* interativos e *apps*) destruiu grande parte dos mercados de transportes e táxis (*Uber* e similares), telefonia (*Skype*, *WhatsApp*...), comércio presencial (com entregas como *Rappi*, *Uber Eats* e *iFood*) e até de imóveis comerciais (com telemedicina, teletrabalho e escritórios virtuais); e a *web* 3.0 (inteligente e descentralizada) iria igualmente inviabilizar a capacidade de governos de proibir ou interromper a oferta de serviços e produtos pela Internet, vez que o Uber pode ser fechado ou interrompido em uma jurisdição, mas não o Bitcoin e o *Arcade City*[82].

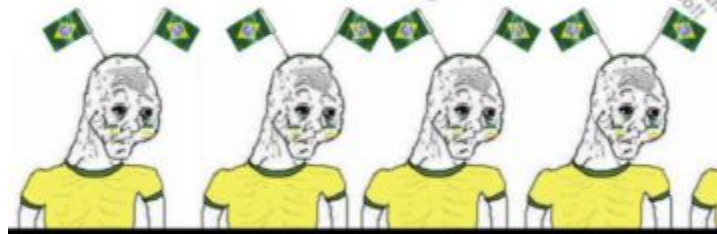
Com a substituição de *smartphones* por *wearables* (dispositivos vestíveis), é possível que o governo veja e ouça mais do que as pessoas veem e ouvem em seu meio (com câmeras nos óculos de realidade aumentada ou virtual – *AR/VR*). Com a popularização do uso da Internet, *Big Data* e *Machine Learning*, grandes empresas têm poder de interferir na opinião pública e eleições (como no escândalo da Cambridge Analítica e nos diversos escândalos que comprovaram que *Facebook*, *Google*[83] e outras empresas têm compromissos íntimos com grupos de extrema-esquerda[84]).

Com o fim das moedas alodiais, novos níveis de totalitarismo e controle são iminentes[85] – inclusive, permitindo juros ainda mais negativos e mais gasto estatal. Se o mundo futuro será um paraíso regulatório e fiscal comparado com o presente, ou se será um inferno totalitário, depende das ações que tomarmos hoje – inclusive, por meio da divulgação do Bitcoin e do desinvestimento do *legacy*. Essa foi a maior motivação para escrever esta obra.

Pouco ou nada importam as boas intenções de qualquer governante. Como se diz no ditado popular: “de boas intenções o inferno está cheio”[86]. Como já foi comprovado por Hayek em *O caminho da servidão*[87], uma vez adotado o Estado Social (*Welfare*), o caminho para o colapso é inevitável.

Para terminar o prólogo, é necessária a demonstração (corolário) do quão frágil e improvável qualquer melhora pelo voto, em uma breve digressão sobre o governo que seria oposição a tudo que estava posto até então:

IMPOSTOR E TRAIDOR
Bolsonaro não só não cumpriu a promessa de livrar as escolas da doutrinação e da ideologia de gênero, como boicotou a única iniciativa da sociedade que combatia essas práticas, e agora, para completar a traição, sancionou uma lei que oficializa a engenharia social feminista em todas as escolas brasileiras.

11 Comments 8 Shares

Bolsonaro foi eleito com as principais promessas de combater o desarmamento e o comunismo, desaparelhar a Administração e reduzir o Estado. Após eleito foi usualmente referido como “bonobo”, “broxa”[88] e “maior traidor e covarde dos 500 anos" por diversas personalidades que apoiaram e financiaram sua eleição, por não ter desnazificado[89] a Administração, permitindo a explosão da corrupção[90], desmoralização, emissão de moeda e dívida e até mesmo a queda de produção e consumo de energia anos seguidos[91], com "fuga de cérebros sem precedente[92].

Alguém ventilou outro dia que Bolsonaro teria sancionado a Lei Cavalo de Tróia porque está de olho no voto das mulheres em 2022. Bem, se isso for verdade — isto é, se Bolsonaro realmente entregou nossos filhos e netos nas mãos das feministas que infestam nossas escolas, em troca do voto das mulheres —, então, meus amigos, não há nenhum limite para o que esse homem é capaz de fazer para continuar no poder.

Duas frases que se provaram verdade foram: "vamos tomar o poder, que é diferente de ganhar a eleição”[93] e “o Poder Judiciário não vale nada, o que vale são as relações entre as pessoas” – do ex-presidente réu criminal (des)condenado que restou impune, sem passar um dia sequer em cadeia real[94].

Bolsonaro prometia privatizar e reduzir gastos públicos e tributos, flertando com imposto único, fechamento do STF, cortes de “bolsas-vagabundagem” e armamento de fuzil para fazendeiros. O resultado após a maior parte do mandato foi:

1) ampliou o desarmamento, reduzindo o número e a natureza das armas que um cidadão comum pode ter no SINARM (sistema de registro de armas de cidadãos comuns), indicando para o MJ - Ministério da Justiça sucessivos agentes admiradores e ativistas da extrema-esquerda, que, por sua vez, aparelharam o MJ com desarmamentistas convictos[95];

2) no Ministério da Fazenda, como na maioria dos ministérios, indicou majoritariamente esquerdistas e gente comprometida com a extrema-esquerda – como a nomeação da família de Leo Pinheiro (um dos principais operadores do mensalão) para a CAIXA; de Gustavo Franco (íntimo de FHC e #elenão ativo na época da eleição) e Levy (ligado e indicado por Dilma e que estava no jantar de Cabral em Paris) para o BNDES; e de gente

do BTG (cujo controlador é ex-presidiário por ser “o banqueiro de Lula”) para a maioria dos bancos públicos;

3) nas mudanças legais, ampliou os privilégios feministas[96], a engenharia social e a carga tributária, reduzindo a poupança e a renda privada com uma reforma da previdência imoral e estatista que pereniza a miséria;

4) o ENEM de 2019 foi amplamente considerado o mais vergonhoso, em sua desorganização, e progressista, em seu conteúdo, desde sempre[97] - e o de 2020, nem se fala;

5) em vez de combater o comunismo e cortar relações diplomáticas com ditaduras criminosas, Jair prometeu, em discurso na ONU[98], facilidades como o ingresso no país sem visto de agentes do regime mais assassino e genocida da história, enquanto seu vice propunha abertamente casamento do país com o Partido Comunista Chinês (PCC); e,

6) em vez de eliminar estímulos perversos[99] de “bolsas-farelo petralhas”, que subsidiam o ócio e a informalidade, sancionou o maior programa de subsídio à vagabundagem com “Auxílio Emergencial” a mais de 66 milhões de pessoas[100] (excluindo qualquer empregado ou servidor) e, em ano eleitoral, propôs “imposto de renda negativo” para perpetuar esses pagamentos.

Resistir é desinvestir! Ter qualquer coisa em ditadura de exceção bolivariana é financiar e apoiar seus crimes. Quando o voto na urna é opinião da maioria são irrelevantes, relevantes passam a ser os “votos com os pés” (onde coloca o dinheiro) ou com armas (lutando para reconquistar as liberdades).

Os Estados Sociais hoje são deficitários (como previsto por Hayek) e não são sustentáveis. Eles tendem a se transformar em:

1) ditaduras totalitárias – como a China[101], com seu Estado policial com monitoramento e controle draconiano e milhões de vítimas em campos de concentração para retirada de órgãos[102] por crimes políticos, como ser cristão ou islâmico; ou 2) paraísos regulatórios e fiscais de portas abertas ao Bitcoin, seja vendendo cidadania sem imposto de renda (*St. Kitts*), residência com isenção perpétua (Zug) ou outros benefícios, como Gibraltar, Curaçao, Malta, Estônia, Paraguai, Portugal, Coreia do Sul, Japão ou El Salvador.

Desde a Antiguidade Clássica até os pais fundadores, reconhecia-se que a democracia é uma degeneração da República – tanto que nem empregaram o termo em sua Constituição, única a durar mais de dois séculos, com exceção da de San Marino. Tanto é uma corrupção da ideia da sociedade pública no "condomínio em que os porteiros votam" que a Coreia do Norte e a Alemanha Oriental, apesar de suas experiências criminosas, tinham "democrático" em suas denominações oficiais.

Hoppe demonstra que "a democracia virtualmente garante que somente os maus e perigosos cheguem ao topo do governo", o que é comprovado nos casos de redução do Estado com explosão de riqueza e desenvolvimento em Hong Kong, Coreia do Sul e Cingapura. Isso não ocorreu onde havia democracia – mas, sim, legalidade e garantia de direitos à propriedade.

Também é demonstrado há décadas – tanto pelas escolas de economia política do *Public Choice* (Teoria das Escolhas Públicas) e de *Bloomington* – que é categoricamente impossível regenerar Estado de Exceção totalitário por vias institucionais e tampouco sem eliminar as "elites dirigentes" ou "grupos concentrados de interesse", como demonstrado no "Problema de Olson" (ou problema da ação coletiva). Para eles, as únicas alternativas a ditaduras de exceção são: votar com os pés (desinvestir e migrar); votar com armas (matar e arriscar-se a morrer); ou enfrentar a submissão, o terror e a miséria. Como todo confronto em que não há chance de acordo, as opções são fuga, luta ou submissão.

> *[Bitcoin é] muito atraente para o ponto de vista libertário se pudermos explicá-lo corretamente. Eu sou melhor com código do que com palavras.*
> Satoshi Nakamoto

É mais fácil o macaco mudar de árvore ou mudar a árvore de lugar?

Salvar a si mesmo é muito mais fácil que terceirizar a responsabilidade (terceirização moral) de salvar a sua família ou garantir seu sustento na velhice esperando um salvador da pátria ou melhorias institucionais que não ocorrerão. É assumir sua responsabilidade e fazer seu *hedge* ou *shortar* abertamente o que aponta para queda iminente. Aí,

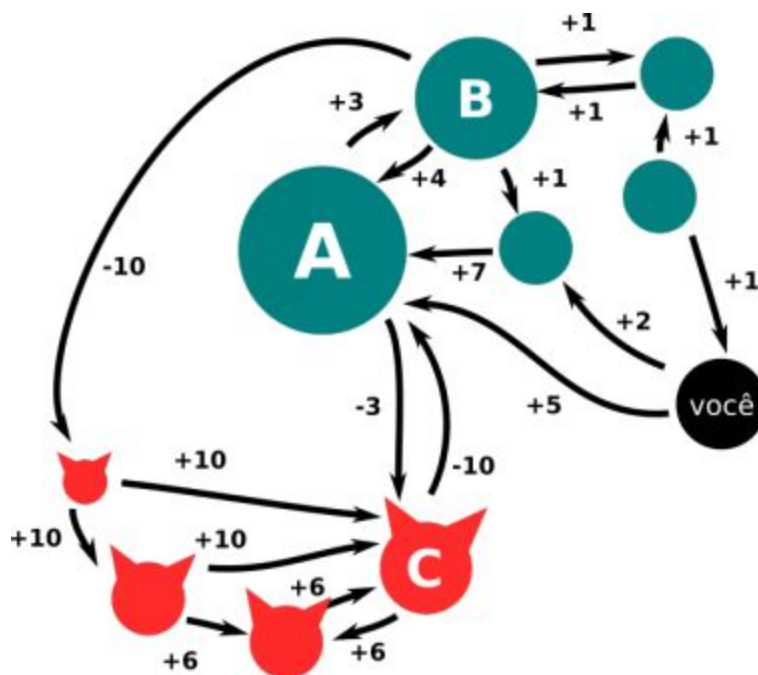
restam o lucro e a tranquilidade, mesmo ao ouvir os absurdos da mídia oficial ou dos políticos eleitos.

A utilidade da informação não é perdida quando partilhada, por isso, PI (Propriedade Intelectual) é roubo[103] (sua natureza é violenta, vez que a única maneira de impor esses direitos é involuntária, por monopólio não contratual). Sinta-se à vontade para reproduzir parcial ou totalmente a obra, contanto que referencie a fonte.

Em uma lista de personalidades relevantes na comunidade, para busca de mais conteúdo, não podem faltar: Fernando Ulrich e Safiri Felix[104], grandes *speakers* de Bitcoin que produziram conteúdos muito didáticos para iniciantes. Richard Rytenband também tem excelentes materiais, como a série “Os Antifrágeis”, explicando a obra de Nassim Taleb capítulo por capítulo.

Há canais de resumos de notícias[105], como: “Visão Libertária”; Ideias Radicais (ressalvado que já elogiou a Atlas, pirâmide descarada e apaga vídeos quando muda de opinião[106]); Investidor Libertário (Roberto Pantoja); e KoreacomK[107] . Quanto a AT[108] (análise técnica), os principais atores em português são Guilherme Rennó e Fausto Botelho, acertam mais que erram, mas ambos já foram “oprimidos". Os “Bitcoinheiros”[109] são maximalistas de alto valor e reputação. Número de seguidores e *views* não são medidas de qualidade na Internet[110]: diversos golpistas e piramideiros têm centenas de milhares de seguidores - inclusive o *YouTube*, há anos, lucra com crimes e golpes anunciados na plataforma.

Há entes mais antigos na comunidade e com muito mais conhecimento técnico, reputação e horas dedicadas ao ecossistema que os autores, como Felipe Mica, Rodrigo Souza, Marco Carnut, Algorista, Daniel Fraga e Narcélio Filho. Se tiver dúvida sobre a reputação de alguém, verifique, pergunte a alguém em quem confie, construa sua rede de confiança[111] *(WoT - web of trust)*. Uma das máximas da comunidade é “*don’t trust, verify*” – não confie, verifique. “*Everyone is a scammer, and willpower is your only defense.*”

Rede de confiança (*WoT – web of trust*)[112]

Outras fontes em português recomendadas para quem passou do básico são: o "Café com Satoshi" (relatório quinzenal da Paradigma Capital); o relatório da NOX (além dos cursos de derivativos de João Paulo da Nox Bitcoin); 21 Milhões Podcast (João Grilo); *Foxbit Research* (relatório da Foxbit); Explica Bitcoin (@BitcoinExplica: traduções de artigos gringos sobre Bitcoin) e o portal *Livecoins*.

Em inglês, os principais canais do *Youtube* são: Keiser *Report*, C*ointelegraph*, *Cryptotips, BTC Sessions e Bitcoin Fixes This*, do Jimmy

Song.

Para um nível mais avançado, além das comunidades nas redes sociais, os *podcasts* de Stephan Livera, Laura Shin *(Bitcoin Unchained)* e o PeterMcCormack *(What Bitcoin Did Podcast)*, Anthony Pompliano *(The Pomp Podcast)*, Guy Swann *(Bitcoin Audible)*, Saifedean Ammous *(The Bitcoin Standard Podcast)* que têm crescido mais que os canais de *YouTube* e *Bitchute*. Uma etapa importante na educação em criptomoedas é cursar *MOOCs*[113] (cursos virtuais normalmente gratuitos), como da Universidade de Nicosia, ou o curso sobre Economia Austríaca e Bitcoin, da *The Bitcoin Standard Academy*, de Saifedean.

INTRODUÇÃO
A doença ponerológica e a cura criptográfica

"O futuro não chega para todos ao mesmo tempo." Ainda há pessoas que vivem em casas sem energia elétrica ou água encanada, se locomovem por tração animal e cozinham com lenha.

A criptografia[114] foi considerada arma de guerra por gerações. Entretanto, armas nas mãos de combatentes que não sabem quem é o inimigo, nem em que guerra estão lutando não têm valor algum. Essa introdução detalha algumas das ameaças que justificam o uso da criptografia como bote salva-vidas.

Demonstrações comuns disso são as pessoas que descobriram o Bitcoin cedo, tendo domínio de conceitos de TI, Teoria dos Jogos e até programação, mas que não entenderam suas implicações políticas, econômicas e sociais, perdendo a oportunidade de investir cedo tudo o quanto poderiam e deveriam.

O mundo está passando por uma mudança de paradigmas na produção, circulação e distribuição de riquezas, que alguns definem como Era Digital, Singularidade ou Economia da Abundância[115]. Essa revolução tecnológica, como as anteriores, vai reduzir brutalmente as margens das atividades superadas e promover uma transferência de riquezas sem precedentes.

Atividades que há poucos anos eram de alta tecnologia e retorno hoje sofrem processo de *commoditização* – até na fabricação de *hardware*, telecomunicações e desenvolvimento de *software*. Como resume Michael Saylor: em todas as épocas os melhores negócios são de alta tecnologia, margem está nos mercados ainda não competitivos.[116]

Neste ambiente, as formas convencionais de criar e acumular riqueza não funcionam mais. No passado, bastava gastar menos do que se ganhava e, sistematicamente, investir o excedente em fontes de renda – deixando o juro composto fazer o resto do trabalho.

Hoje não existem mais fontes de renda perpétuas, não existem mais investimentos seguros que garantam fluxos de caixa com retornos positivos sistemáticos e, provavelmente, todos os produtos financeiros convencionais têm expectativas de perda real. Essa disfunção alimenta a ética hedonística do consumismo e a irresponsabilidade, que induz as populações à miséria e ao voto nos estatistas, uma vez que, “quando se quer o impossível, apenas mentirosos podem satisfazê-lo”.

Ora, foi pela falta de acesso a produtos financeiros idôneos a produzir ganhos que, por gerações, os investimentos prioritários do brasileiro (em especial de baixa renda) eram imóveis – para agropecuária no interior e para construção nas áreas urbanas (chegando-se ao ponto de haver mais lojas de materiais de construção que padarias).

Diante da queda da fecundidade e da massificação do comércio digital, as demandas por imóveis residenciais e comerciais tiveram suas tendências comprometidas. A agricultura profissional de pequeno porte se inviabilizou, como consequência da quebra da segurança jurídica no campo (vide ações terroristas impunes do MST – Movimento dos Sem Terra – e desarmamento covarde dos inocentes), da indústria de multas ambientais e da [in]justiça do trabalho.

O que aconteceu com quem vivia de alugar “placas de táxi”? O que aconteceu com a renda de quem alugava linhas telefônicas? O mesmo deve acontecer, cada vez mais rápido, em dezenas de setores – até o final da próxima década (considerando as curvas exponenciais), com os governos, suas moedas fiduciárias e todos os investimentos sob seu controle soberano.

Novas indústrias surgem com tecnologias da *Internet of Business (big data, blockchain, IOT, AR, VR, AI, analytics e cybersecurity)* a ponto de mais de 90% dos ganhos dos índices convencionais de ações dos EUA nos últimos anos serem de empresas “.com”[117] – com ênfase nas *FAANGs* –

com praticamente todos os demais setores tendo suas rentabilidades mitigadas. Isso denota a morte de grandes corporações e declínio de setores inteiros que eram dominantes há menos de uma década.

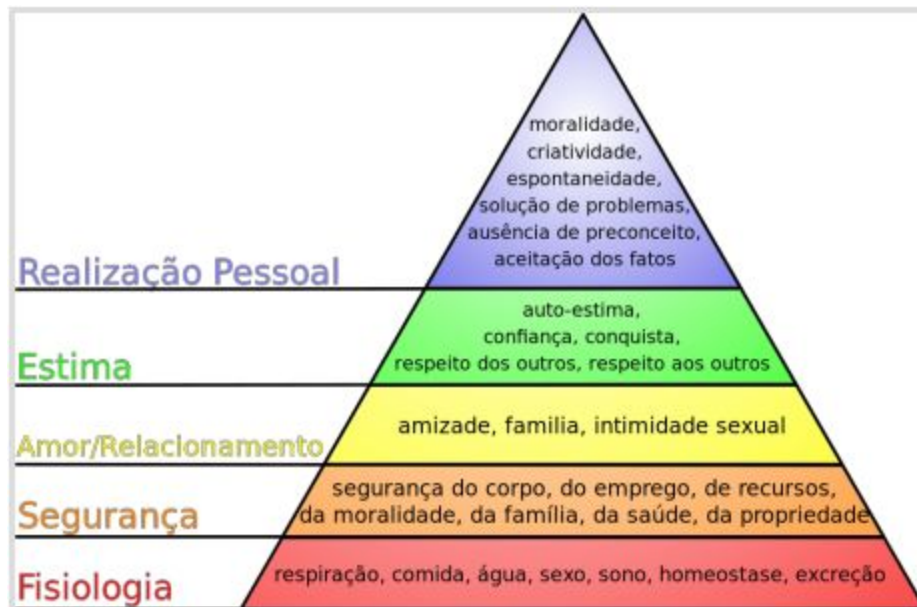
As ações tendem a ser substituídas por *equity tokens*, as moedas fiduciárias de governos por *cryptocurrency*, e sistemas democráticos por democracias societárias e sistemas de consenso ou holocráticos. A riqueza também tende a migrar dos ativos físicos para aqueles imateriais (como conhecimento).

O fim do sistema convencional – *legacy system* – não é evidente apenas na perda de lucratividade e eficiência das empresas tradicionais, mas também no esgotamento dos modelos governamentais, políticos e sociais em face do fim dos poderes estatais que os financiam.

As sociedades ocidentais vivem em crises morais, financeiras e demográficas – evidentes pelos níveis de fecundidade abaixo dos níveis mínimos de manutenção, pelos juros reais negativos, pela "Guerra ao Dinheiro" (com a progressiva ameaça de fim do dinheiro físico e totalitarismo financeiro) e pelo *déficit* sistemático e exponencial dos Estados Sociais (*welfare states*), demonstrando sua insustentabilidade e a iminência de seu colapso.

A pirâmide de Maslow[118] demonstra que, satisfeitas as demandas mais primitivas, novas demandas surgem hierarquicamente para os seres humanos. Quem está sendo sufocado por minutos não vai se preocupar em estar com sede por horas, e quem não tem água por dias não vai se preocupar com a fome.

Na verdade, ganhar dinheiro, ter sexo ou obter aceitação social só é uma grande preocupação nas camadas[119] iniciais da personalidade, ou seja, para aqueles que têm dificuldade de atingir esses objetivos. Quem ler e compreender os objetivos deste livro e ainda não for independente, vai avançar uma camada nesta pirâmide: vai vencer uma preocupação comum para liberar tempo e energia para questões superiores.

Hierarquia das necessidades de Maslow

Compreendendo esse conceito e observando como as prioridades médias da população têm descido para baixo na pirâmide referida, fica claro como a camada da personalidade média da população, o QI e o desempenho em testes de conhecimento informativo[120] têm decaído sistematicamente por décadas no Brasil.

Nenhuma sociedade com QI médio inferior a 90 chegou ao primeiro mundo e – com exceção de lugares que experimentaram o terror comunista – nenhum país com QI médio acima de 100 deixou de se tornar desenvolvido.[121]

As correlações entre baixa preferência temporal[122] (autocontrole de sacrificar benefícios no presente para usufruir no futuro), o alto QI e maior renda são observáveis em indivíduos e em populações, embora haja grande controvérsia entre a causalidade recíproca ou comum[123].

A destruição da inteligência não é o principal problema do país, ela é apenas uma consequência do processo ponerológico que implantou a patocracia[124] e o Estado de Exceção no país. A ponerologia é uma doença mental coletiva promovida pela engenharia social que utiliza o marxismo cultural como ferramenta de infiltração e subversão.

Para quem nunca teve contato com estes conceitos, as estratégias de inteligência dos grupos totalitários podem parecer "teoria da conspiração", mas essa é a explicação simples porque, nas mais diversas áreas do conhecimento e das políticas públicas, teorias e mitos refutados são tidos como verdades científicas e senso comum.

O fato é que as instituições brasileiras são aparelhos marxistas – como tribunais, mídia, academia e até igrejas – porque foram infiltradas e subvertidas por ações de contrainteligência por mais de 90 anos através de concursos fraudados ou enviesados e de assassinatos de reputação ou reais. Primeiro, pelo esforço soviético[125] e, após isso, por seus sucessores como o Foro de São Paulo[126]. Desta maneira, o cultivo da mentira, da falta de inteligência, da corrupção e da miséria foi planejado e executado como ferramenta de engenharia social.

Governos precisam de populações majoritariamente pobres, dependentes e submissas para manter seu poder. Se as pessoas forem independentes, ricas e céticas, elas vão atribuir poderes aos governos? Esta é a razão real de o governo controlar a educação e a moeda.

Evidência de como existe uma brutal diferença entre a verdade e as informações direcionadas para as massas é o indicador de preço que

funcionou com 95% de precisão (se interpretado no sentido inverso): foi a subida do preço do bitcoin quando a CNBC fazia reportagens negativas e a queda quando fazia manchetes positivas[127].

Uma demonstração objetiva de que o crescimento do Estado é uma ferramenta de engenharia social e não ocorre de boa-fé, pelo menos quando há psicopatas no poder, é a violação dos limites das curvas de Laffer e de Rahn[128] pela instituição de alíquotas mais altas que o ponto ótimo de arrecadação.

Como comprovado por extensa literatura, mesmo nos Estados Unidos, os governos poderiam arrecadar mais reduzindo os níveis de tributação e gasto público – mas não o fazem para satisfazer grupos lobistas, devido à captura administrativa.

Outra tendência da engenharia social, ressaltada por autores como Stefan Molyneux[129], como sinal do colapso civilizacional, é o relativismo moral, com ápice nas histerias transexualista, negrista, gayzista, pedófila, zoófila[130] e feminista[131] como pautas relevantes de debate político e com super estímulo à promiscuidade e castração em crianças.

Um dos fatores cruciais que inviabilizou a manutenção da escravidão em sociedades cristãs, embora esse fosse um instituto mencionado e reconhecido na Bíblia, foi a restrição moral à promiscuidade. Escravos que têm relações monogâmicas passam a ter relações conhecidas de parentesco e, formando famílias, passam a ter pessoas dispostas a matar e a morrer umas pelas outras e a ter identidade ancestral.

Por isso, sociedades com quantidades significativas de escravos só conseguiam mantê-los escravos através de esquemas obrigatórios de cobertura por múltiplos parceiros – eliminando as relações monogâmicas e, consequentemente, destruindo o núcleo de proteção e estrutura social básica – como em Roma e na Grécia Clássicas[132].

Autores como Rollo Tomassi[133], Stefan Molyneux[134] e Olavo de Carvalho também ressaltam que um dos fatores-chave para a queda da fecundidade – que sentenciou as previdências de repartição ao colapso – foi a liberação sexual e a instituição de leis subvertidas feministas[135], obliterando as motivações de homens e mulheres para manterem famílias estruturadas[136].

Mesmo bilionários como Saylor simplesmente desistem de casar, estilos de vida como *herbs* japoneses *e MGTOW* são, cada vez mais comuns. A sua argumentação[137] é simples: as leis inviabilizam contratos viáveis de casamento, de modo que governos feministas garantem estímulos ao maximizar o oportunismo hipergâmico. Em outras palavras, o governo é uma máquina de transferir riqueza e poder de produtores (a maioria homens) para dar a beneficiários de renda estatal (a maioria mulheres), como é óbvio pelos dados de pagamento de impostos ou até mesmo contribuições e benefícios previdenciários[138].

Historicamente, o que um homem poderia oferecer como homem era segurança – física, material e emocional – e o que uma mulher poderia oferecer era fertilidade - aferida por atributos físicos - e fidelidade. Por isso virgindade é ativo para mulher e passivo para o homem no cálculo do valor sexual e, de maneira inversa, a promiscuidade[139].

Essa troca ficou inviabilizada com leis feministas atuais, como a absurda e antinatural paternidade involuntária por *DNA*, fomentando o golpe da barriga, promiscuidade[140] e nascimentos fora do casamento - a ponto de Molyneux denominar o *welfare state* como *single mom state*[141], devido a

altíssima correlação entre desestruturação familiar (e moral) e o aumento do Estado Social.

As mulheres não precisam mais de segurança do homem (agora, provida oficialmente pelo Estado, em cada um dos aspectos). Os homens, sem qualquer garantia de fidelidade e com amplo acesso a sexo com custo marginal quase zero, não têm motivação para investir em procriação de filhos[142] sob os quais não terão poder, comprometendo sua renda por décadas e que podem até não ser deles[143].

Segurança física é o que explica as filas de mulheres jovens e bonitas para "visitas íntimas" nas cadeias. Uma vez que sejam mulheres de bandido filiado à facção passam a ser protegidas até mesmo de “talaricagem” no tribunal do crime. Fora do ambiente controlado por facção criminosa assumida, o protetor da mulher é o Estado que faz propaganda afirmando que seu marido ou seu pai é agressor e estuprador em potencial e deve ser denunciado ao Estado.

Segurança material é o homem exercer papel de provedor. Com mulheres ganhando mais e tendo mais instrução que homens, graças à explosão de assistencialismo, distorções e gastos públicos do Estado “gigolô”, as mulheres não precisam mais de provedor.

Dalvana, que isso... na nossa casa...

Deixe de ser machista, Carlos, são novos tempos.
Eu não tolero isso, acabou. Vá embora, a casa é minha.

Alô, polícia? meu marido machista está me agredindo psicologicamente, socorro!

Não resista, cidadão, vai virar putinha na cadeia, machão!
E aí, pessoal do insta, tamos aqui agora prendendo esse machão agressor de mulher, arrasta pra cima!

Ainda pior, com mais instrução e renda, a mulher tende a se avaliar muitos pontos acima do seu real valor sexual de mercado[144], ficando alienada (na busca por relacionamentos, mesmo conseguindo muitos parceiros sexuais), por nunca encontrar um par que ela julga digno para compromisso (e que a aceitaria). Ainda pior quando é enganada pela promessa de estabilidade de “previdência”, “cargo público" ou "herança".

Essa é a gênese usual das “tias dos gatos” e das “mães de *pets*”[145].

Humanos também são animais, seus comportamentos têm aspectos evolutivos etnobiológicos[146] consolidados em milhares de anos de pressões seletivas: homens serem homens, mulheres serem mulheres e humanos serem seres gregários e tribalistas. Quando normas jurídicas inviabilizam o exercício dos comportamentos naturais — contrariando o direito natural e o PNA[147] — as famílias, comunidades e países se degeneram — com destruição das instituições, queda da fecundidade, diluição da moeda e da moral[148]:

Por isso, os governos e corporações estimulam a degeneração dos valores morais e éticos, por meio de leis de alimentos e pensões, bolsas assistencialistas (que não permitem ascensão dos mais pobres, mantendo-os eternamente na pobreza), privilégios a grupos de poder (incluindo minorias intolerantes) e campanhas “culturais” subversivas[149]. A finalidade é única e simples: obter mais e mais votos e ativistas para partidos de extrema-

esquerda, alimentando o ciclo de mais impostos para os produtores e mais auxílio aos parasitas.

Outro exemplo da histeria e infantilização coletiva usadas em prol de interesses corporativos e estatais é a preocupação com falsas questões ambientais, como na década de 1980, com o "buraco na camada de ozônio", ou a mania atual do "aquecimento global", rebatizado para "mudanças climáticas" – desmoralizada recentemente pela descoberta de processos como o "escurecimento global"[150].

Ora, sobram evidências de que a Terra já foi muito mais quente e mais fria, muitas outras vezes; e, havendo ou não havendo "mudanças climáticas", a sociedade vai se adaptar muito melhor sem regulações estatais do que com elas[151].

Ademais, os maiores desastres ambientais da História provocados pela humanidade foram causados por Estados totalitários[152] e não por empresas – vide Chernobyl, Kyshtym[153] e o Mar de Aral na URSS, e a grande ideia de Mao Tsé-Tung de matar pardais (Campanha Mate um Pardal), provocando a grande fome na China[154] – a ditadura comunista é campeã atual em qualquer tipo de passivo ambiental[155].

O Efeito Gell-Mann de Amnésia[156] ilustra como pessoas altamente instruídas aceitam fontes refutadas por elas mesmas, desde que em temas nos quais não sejam especializadas.

Desde Hayek (para não dizer desde os *founding fathers*), qualquer jurista de respeito entende que só existem direitos públicos negativos[157] e promessas de saúde e educação públicas são o "caminho da servidão", levando inevitavelmente ao totalitarismo. Qualquer médico ou nutricionista com formação mínima sabe que os mitos – acerca das gorduras saturadas, sal e fibras – difundidos por Ancel Keys são mentiras descaradas[158]; como afirmações de que pecuária é prejudicial ao meio ambiente[159], qualquer economista decente entende que o "ambiente intelectual" de keynesianismo e marxismo só leva a mais estatismo, subdesenvolvimento e pobreza. Agora, cada um deles, embora entenda que o "senso comum" ou "discurso convencional" sobre sua área seja um monte de mentiras refutadas, ainda tende a dar crédito pleno às mesmas fontes (academia, mídia, governo...) nos demais temas.

O grupo de *Cypherpunks* no qual o Bitcoin começou já compreendia o entendimento de Hoppe de que a *Democracia é o deus que falhou*. Na

verdade, há muitos exemplos de democracias funcionais – como as societárias –, embora até mesmo os *founding fathers*[160] tivessem ojeriza a este termo, evitando-o na Constituição Americana e utilizando o termo "República". Assim como a adoração pelo termo "democracia" por ditaduras totalitárias e assassinas como a "República Popular **Democrática** da Coreia" (Coreia do Norte) e a "República **Democrática** Alemã" (Alemanha Oriental).

Uma democracia em que os beneficiários líquidos (parasitas em linguagem ecológica) votam e têm maioria é como um condomínio em que os porteiros e visitantes votam.

Ora, os porteiros e visitantes, que não pagam condomínio, vão sempre votar para que sejam ampliados seus benefícios e as taxas condominiais – até que as unidades percam todo o seu valor e o condomínio quebre. Esse é o resumo do que é um Estado Social e por que todas as experiências de dar saúde e educação "gratuitas" sempre terminaram em tragédia, terror e miséria desde a República de Weimar até a atual colonização da Europa pelo Islã – através dos *welfare magnets*, que impõem a *sharia* e sua cultura de violência e estupro sistemático de mulheres ou crianças "infiéis".

Nassim Taleb[161], em sua obra magna *Skin in the game*, demonstra os riscos inerentes à dissociação do controle e propriedade — e da tomada de decisões sem a assunção de consequências.

Essa dissociação já era demonstrada, há gerações, como a causa primária da corrupção na Teoria da Agência e na compreensão dos axiomas de Klein e Jensen-Meckling (contrato e dos agentes imperfeitos), mas eles ainda não permearam o "ambiente intelectual" o suficiente para que haja o entendimento corrente de que a única maneira de reduzir a corrupção e promover o desenvolvimento é reduzir o Estado e seus poderes.

As pessoas respondem a motivações, como demonstrado por Douglass North[162] e outras fontes da Economia Institucional: o que faz um país ser desenvolvido ou subdesenvolvido são suas instituições; sistemas em que comportamentos dominantes são oportunistas levam à corrupção endêmica e ao subdesenvolvimento. Por outro lado, onde há governança privilegiando a cooperação como comportamento dominante, tem-se desenvolvimento.

O Bitcoin possibilita que pessoas que vivem em qualquer país, por mais corrompido e subdesenvolvido que seja, possam usar uma reserva de valor e meio de pagamento capaz de mudar suas motivações em relação a

preferências temporais. Isso pode levar o mundo a uma nova era de produtividade e progresso – material, ético e tecnológico.

Ammous[163] também explica detalhadamente que a decadência das artes, inteligência, moral, famílias, impérios e até da saúde mental das populações é altamente correlacionada com a ausência de *sound money* – dinheiro sonante, capaz de ser reserva de valor – e de baixas preferências temporais decorrentes dele.

Então, se o leitor quer investir em alta cultura e considera que a guerra cultural é a primeira a ser vencida, entenda que o primeiro passo para isso é a adoção de uma boa reserva de valor que mude as motivações e, consequentemente, reduza as preferências temporais. E, o segundo passo, é o desinvestimento dos ativos que o leitor tem no domínio do inimigo, o *legacy*.

Para um país, uma empresa, uma família ou um indivíduo, os elementos fundamentais para a determinação de crescimento são acumulação e produtividade. Por motivos óbvios, no Brasil, os níveis de produtividade em relação ao resto do mundo e os níveis de poupança apresentaram quedas sistemáticas nas últimas décadas – e com o envelhecimento da população e a deterioração das instituições, a tendência é piorar.

A produtividade é determinada por diversos fatores – inclusive tem significativa correlação com poupança; mas um determinante simples dela em populações é o QI[164]. Poupança também é submetida a diversos fatores, mas o que pode servir de preditor imediato são as preferências temporais[165] baixas.

Só para dar um exemplo de como o Brasil é um país improdutivo: segundo dados oficiais[166], menos de 25% das terras são produtivas (somando cidades, agricultura, infraestruturas e pecuária) – enquanto a maioria dos países desenvolvidos empregam mais de 75%. Para piorar, no caso de “Banânia”, mesmo nesta fração útil, a produtividade ainda é baixíssima, com pouco uso de mão de obra (inviabilizada pela legislação trabalhista engessada) e tecnologias de ponta (inviabilizada pela regulação e tributação sufocantes).

Os níveis de eficiência e produtividade da utilização da mão de obra não são melhores (dados os níveis absurdos de inatividade, como os *nem-nem*[167] – nem trabalha e nem estuda –, eternos estudantes e desempregados) e tendem a piorar com o envelhecimento.

É uma demonstração de ignorância ou má-fé pessoas advogarem por determinação da taxa de juro pelo governo ou pela redução da taxa SELIC para estimular a economia. Ora, o brasileiro que viveu os congelamentos de Sarney e que testemunhou as experiências semelhantes de Maduro na Venezuela sabe muito bem quais as consequências do controle de preços – escassez e miséria. Governo determinar taxa de juro é imoral e economicamente pior que tabelar o preço do pão ou do feijão, pois se pode viver sem pão ou feijão (existem substitutos), mas não se pode viver em uma sociedade com curso forçado sem tocar em moeda estatal.

Se o governo pretendesse realmente reduzir as taxas de juro para fomentar a atividade econômica de maneira sustentável, ele iria cumprir suas funções próprias (jurisdição e defesa), aumentando e facilitando os meios de defender a propriedade privada e de executar devedores.

Desta forma, é importante frisar que consumo não produz crescimento sustentável, investimento sim. Maior consumo significa menor investimento – ou seja, menor produtividade futura.

Acumulação e propriedade não devem ter "função social" além de satisfazer as preferências do dono. Até mesmo Jesus, na Parábola dos Trabalhadores das Vinhas[168], deixa claro como é má e pecaminosa a pretensão de regular contratos voluntários alheios como faz a legislação trabalhista.

Quando alguém utilizar expressões como "função social", "empoderamento", "politicamente correto", "todes", "tod@s" ou "apropriação cultural", já se pode identificar uso da novilíngua marxista para conquistar corações, mentes e, é claro, poder – aquele texto estará reproduzindo linguagem ponerológica de maneira instrumental para desinformação.

Desta maneira, os idealizadores do Bitcoin compreenderam que, o início dos processos de *QE*, "alívios quantitativos", representava o passo final de captura administrativa das corporações sobre os governos, e, em consequência, a última chance das populações de evitar o totalitarismo financeiro com o fim do dinheiro físico e das chances de enriquecimento pela acumulação honesta.

Como demonstrava Bastiat no século XIX, ou Ron Paul no século XX, todas as funções dos Bancos Centrais são mais bem desempenhadas por instituições privadas (ou por ninguém). A emissão de dinheiro é uma

questão importante demais para ser deixada na mão de políticos, assim como a educação[169].

Rothbard[170] ilustra outro aspecto da subversão dos valores morais com o "educacionismo", o mito de que as pessoas devem crescer na vida através da instrução formal, controlada e financiada por governos que aparelham as "escolas" com agentes de doutrinação e manipulação – os *intelectuals yet idiots*, de Taleb.

O aumento exponencial do Estado – usando como justificativa mais regulações para resolver falhas regulatórias anteriores (Lei de Michels[171]) até criminalizar todos na sociedade – dá ao governo o poder de punir quem quiser a qualquer momento legalmente[172]. São políticas com fito de provocar emigração de dissidentes (efeito Curley[173]) e a "Estratégia Cloward Piven" (aumentar obrigações financeiras do governo para provocar o colapso do país e a inevitável adoção de totalitarismo).

Se o Bitcoin sobreviver por mais uma década, ele será um bote salva-vidas para todos esses processos. É o mecanismo de proteção (*hedge*) fundamental contra os processos de insanidade coletiva, corrupção, totalitarismo e endividamento endêmicos; e, por isso, é elemento fundamental em qualquer carteira – não apenas por ser imperativo moral, mas para evitar risco de cauda (risco de ruína perdendo tudo quando o sistema convencional colapsar).

Por isso, até Taleb reconheceu que "o Bitcoin é o início de algo grandioso: uma moeda sem um governo, algo necessário e imperativo".

Como será a seguir demonstrado, o Bitcoin muda as motivações de seus usuários, alonga suas preferências temporais, faz explodir sua produtividade e capacidade de acumulação e, se continuar seu curso de adoção exponencial, pode salvar o mundo do coletivismo – instaurando um novo entendimento do dinheiro e da moeda, da ética do trabalho, acumulação e relação com governos, e de respeito aos direitos alheios, superando mitos, mentiras e instituições corrompidas que atrasam o desenvolvimento da humanidade.

O Bitcoin será morto ou será a *causa mortis* dos Estados Sociais[174] – com a vitória do indivíduo sobre as ditaduras e corporações corruptas. Para isso que foi concebido.

Não é possível manter sob escravidão pessoas armadas e determinadas a serem livres, como Massada demonstrou. Satoshi expressou isso ao afirmar que "em algumas décadas, o subsídio será muito pequeno e as tarifas de

mineração serão a principal remuneração pelos nós de mineração. Estou certo de que em 20 anos haverá um volume de transação muito grande ou nenhum volume”. É vencer ou morrer.

Quando a maior parte da riqueza não puder ser expropriada, controlada ou mesmo ter titularidade suspensa por governos ou tribunais, não haverá como recolher tributos involuntariamente. Penas ou multas, e a ação estatal involuntária não terão mais sentido, viabilidade ou efeito prático.

Com o aumento exponencial dos dados e poderes acumulados por governos e corporações, o mundo se encontra às vésperas de um meio-termo entre as distopias descritas em *1984* e *Admirável Mundo Novo*. Quem quiser evitar viver o drama da *Revolução dos Bichos* terá que se evadir da fazenda antes das fases finais da Revolução – e o Bitcoin é uma das tecnologias úteis para evitar o domínio totalitário e para facilitar a fuga de onde o totalitarismo não possa ser evitado.

É uma guerra de extermínio. A cultura vencedora deste *fork*[175] social será o modelo a ser perpetuado nas futuras gerações. Não tem acordo ou meio termo, não tem prisão nem rendição. Você será livre como nunca sonhou ou escravo como ninguém nunca foi.

CAPÍTULO I: *5W2H*

Septen circuntantiae: *Quis, quid, quando, ubi, cur, quem ad modum, quibus adminiculis*. (*Who, what, when, where, why, in what way, by what mean*s.)

Em qualquer investigação, há um conjunto inicial de questões a serem respondidas ao investigar qualquer fato, *5W2H*: *Who, What, Where, When, Why, How, How Much* – derivadas das sete questões aristotélicas difundidas por São Tomás de Aquino. Vamos às respostas objetivas:

1 (Who/Where/When) - Quem criou o Bitcoin, onde e quando:

O Bitcoin foi proposto em um artigo *(Bitcoin: a Peer to Peer Electronic Cash System*[176]) enviado por um participante[177] que utilizava o pseudônimo de Satoshi Nakamoto (2008) em um grupo de *e-mails* de *cypherpunks*. Em 18 de agosto de 2008, o domínio bitcoin.org foi registrado, em 31 de outubro, o *whitepaper* publicado e, em janeiro de 2009, o código aberto foi divulgado, momento em que o sistema começou a rodar, com a mensagem *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"* registrada no primeiro bloco em 3 de janeiro de 2009.

Nesse grupo, congregavam os principais *cypherpunks*, *experts* em criptografia e ativistas do austro-libertarianismo e, em decorrência disso, o espaço era utilizado por alguns de seus participantes como meio de divulgação e teste de *softwares* abertos e descentralizados, em grande parte como resposta aos abusos reincidentes por parte dos governos dos seus privilégios de senhoriagem e monopólio de emissão de moeda. Os integrantes desse grupo sabiam que o domínio da criptografia pelo indivíduo médio era um fator fundamental para evitar o totalitarismo, como fica claro no *Manifesto Cripto Anarquista*[178], de Timothy C. May.

Os austro-libertários, como diversos grupos liberais clássicos e conservadores, até o desenvolvimento do Bitcoin, sempre defenderam o *gold standard*, o princípio de limitação da emissão de moeda às reservas de ouro de cada país, que evita inflação e preserva o valor da moeda corrente.

Usualmente, as civilizações em colapso acompanharam políticas destruidoras de valor, como tabelamento de preços e *déficit* sistemático, que

só foram possíveis por meio da diluição do valor da moeda, desde o Édito Máximo de 301 A.D. (homólogo à tabela da SUNAB em Roma), com a diluição exponencial dos denários desde Diocleciano e Nero até as práticas semelhantes nos governos de Nixon, Sarney, Kirchner, Maduro e Chávez.

> O problema raiz da moeda convencional é toda a confiança necessária para fazê-la funcionar. O Banco Central deve ser confiável para não desvalorizar a moeda, mas o histórico das moedas fiduciárias está cheio de violações dessa confiança.
>
> Satoshi Nakamoto

Após propor o *whitepaper* e contribuir ativamente na comunidade nos primeiros anos, Satoshi Nakamoto se despediu e deixou o projeto que continuou de maneira descentralizada[179]. Os primeiros bitcoins minerados, supostamente por ele, não foram movidos – servindo de prova de segurança das carteiras mais modernas e de garantia de que o criador até hoje não obteve vantagem pecuniária pela venda dos primeiros *tokens* criados.

Em que lugar fica o Bitcoin? Todos os registros de transações se encontram em cada nó (*full node*)[180], que totalizam mais de 10 mil usuários com o cliente instalado (*nodes ou nós públicos*)[181]. Desta maneira, o Bitcoin não está em nenhum país ou jurisdição específica, mas, sim, nas nuvens[182]. Um ótimo artigo chamado “A fabulosa ilha Bitcoin”[183] (2015), escrito por Felipe Micaroni, explica muito bem o processo de forma didática e lúdica.

Uma ordem monetária espontânea emerge das interações complexas; não é algo conferido por debate acadêmico, planejamento racional ou mandato do governo.

Saifedean Ammous

2 (What) - O que é o Bitcoin

Em apenas uma frase: bitcoin (*token*) é o dinheiro que pode ser enviado por qualquer meio de comunicação[184] e Bitcoin é o sistema público e aberto de registros de seu *token* nativo e o *software* livre para sua utilização pela Internet.

Por isso se afirma que para proibir o uso de bitcoins, globalmente, seria necessário destruir a Internet em todos os países do mundo; ou, em uma jurisdição determinada, impedir o direito de expressão, retirando dessa população rádio, *SMS*, telefone, carta e qualquer outra forma de comunicação com pessoas quem tenham acesso à Internet.

Direito com “D” maiúsculo é o sistema jurídico, conjunto de normas; e direito com “d" minúsculo é a faculdade legal. De maneira análoga, Bitcoin com “B" maiúsculo é uma plataforma, constituída de um *software* aberto e livre, com milhares de atores validadores e processadores (nós e mineradores) em um sistema de registro descentralizado[185] denominado *blockchain* ou *timechain;*

Esse sistema já consome mais energia que vários países e possui o maior poder de processamento do planeta — cerca de 89 milhões de *terahashes* por segundo (TH/s) em maio de 2021, cerca de 100 vezes maior que os servidores do Google.

O Bitcoin como sistema é composto por: a) **nós (nodes)**, atores que mantêm os registros das transações passadas (memórias registrando e validando todas as transações); b) **mineradores**, processadores remunerados com os novos bitcoins (subsídio) e taxas voluntárias (*fees*) por disponibilizar poder computacional para processar transações e garantir segurança da rede; e **c) usuários** (entes que usam o sistema, enviando e recebendo saldos)[186]:

Money Over Internet Protocol

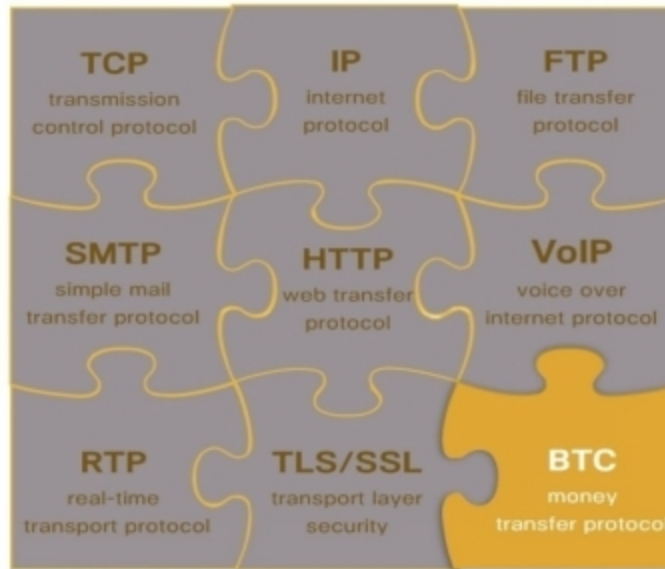



Image from Pantera Capital

O bitcoin com “b” minúsculo é a unidade básica do sistema (*token*), com a qual são pagas taxas (*fees*) para uso e com a qual os serviços de mineração são remunerados. O bitcoin é o “dinheiro digital”, “ouro 2.0”, “dinheiro mágico da Internet”, moeda sem terceiro de confiança (sem garantia de Estado, Banco Central, empresa, *CEO*, nem servidor central), baseada não em entes, mas na confiança em motivações no sistema descentralizado de governança e no *software* proposto por Satoshi Nakamoto[187], operacional há mais de 11 anos.

O Bitcoin tem três funções inatas: a) é sistema de comunicação global, incensurável, público e perpétuo – que garante a faculdade de troca de informações e registro público de dados fora de qualquer controle estatal; b) é sistema de pagamentos que não está sujeito às jurisdições nacionais, o que inviabiliza, na prática, controles de capitais (incluindo no mercado internacional os bilhões de indivíduos sem acesso a serviços bancários); e c) é plataforma de manutenção de saldos como reserva de valor, que apresenta certas características de dinheiro superiores ao ouro e a qualquer reserva de valor anteriormente adotada – libertando seus usuários de expropriações e tributos involuntários, mesmo após a sua morte, incluindo aí até mesmo a senhoriagem e a inflação.

Fernando Ulrich[188], em 2014 e 2015, publicou no *Infomoney* dois textos fundamentais para a popularização no Brasil: *Dez formas de explicar o que é Bitcoin*[189] e *Guerra ao dinheiro, juros negativos e a crise na Grécia*[190].

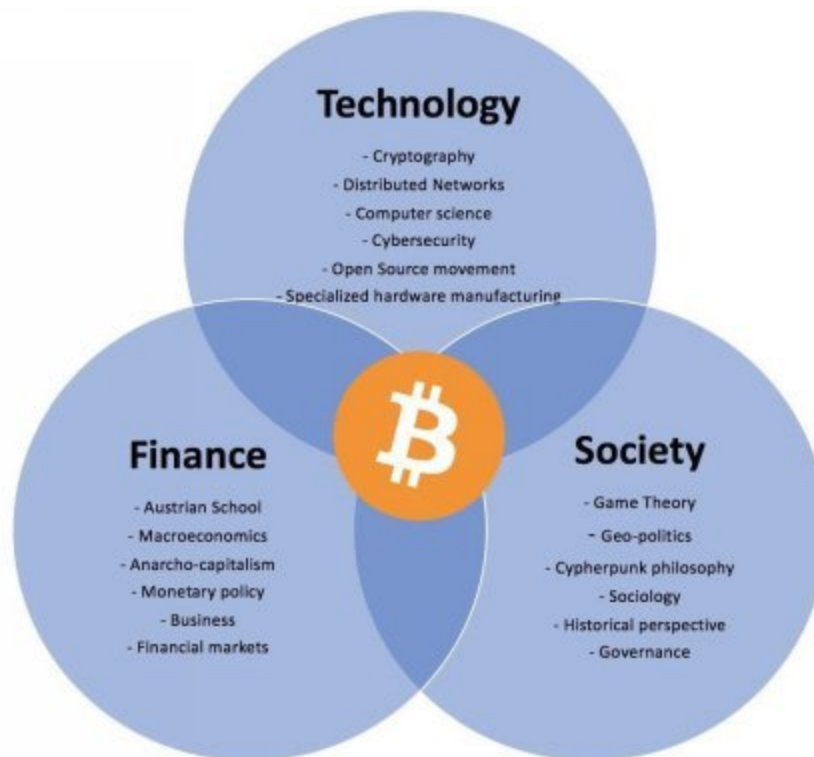
O Bitcoin não é uma democracia. Ele utiliza um padrão de governança superior de decisões por unanimidade em que não há sanções violentas, mas apenas motivações baseadas em Teoria dos Jogos e Teoria das Escolhas Racionais. Essas características o tornam sistema dominante para comportamentos cooperativos e inibem financeiramente o oportunismo[191].

Satoshi[192] demonstra que “a quantidade é uma qualidade em si mesma", quando define o bitcoin como uma mercadoria que tem potencial de valor derivado da raridade e da transportabilidade. Em livre tradução:

> Como um experimento mental, imagine que houvesse uma base metal tão escassa quanto o ouro, mas com as seguintes propriedades: cor cinza; não é um bom condutor de eletricidade; não é particularmente forte, nem dúctil ou facilmente maleável; não é útil para nenhuma finalidade prática ou ornamental, mas tem uma propriedade mágica especial: Pode ser transportada por um canal de comunicação. Se, de alguma forma, adquirisse algum valor por qualquer motivo, qualquer pessoa que desejasse transferir riqueza a uma longa distância poderia comprar um pouco, transmiti-lo e pedir ao destinatário que o vendesse.

Satoshi também deixa claro nos fóruns, no *whitepaper* – e não apenas no Bloco Gênese – que o Bitcoin foi criado para a eliminação dos problemas do terceiro em pagamentos digitais e da degradação da moeda convencional. Em livre tradução:

> Eu desenvolvi um novo sistema de *e-cash P2P* de código aberto chamado Bitcoin [..] – completamente descentralizado – nenhum servidor central – sem partes confiáveis – baseado em prova de criptografia em vez de confiança – problema com moeda convencional é [degradação]...

Como ilustrado[193], o Bitcoin é uma combinação de várias tecnologias e conceitos: Economia – Teoria Monetária – Teoria dos Jogos – Criptografia – Computação – Redes distribuídas e outras, como fica demonstrado no *whitepaper* escrito pelo idealizador, Satoshi Nakamoto:

Como demonstrado por Parker Lewis, a compreensão do Bitcoin é um processo lento, assim como a construção de uma infraestrutura, em um ciclo virtuoso ilustrado pelo esquema[194]:

Conhecimento → Infraestrutura → Adoção → Valor → Conhecimento → Infraestrutura

Logo que o usuário iniciante, *noob*, entende o que é o Bitcoin, algumas questões acerca de sua natureza são típicas: bitcoin é pirâmide? Qual o lastro do bitcoin? Bitcoins vão substituir totalmente as *fiats* (moedas estatais)? O Bitcoin não foi hackeado ou fraudado? Será destruído pela computação quântica? Quando eu morrer, para onde irão meus bitcoins? Era vantagem comprar no início, não agora! Não é melhor comprar a *shitcoin* que custa apenas 1 satoshi em vez de bitcoin?

Pinned Tweet
Willy Woo @woonomic · Jun 13
Fiat: 48.8 years old
Bitcoin: 11.4 years old
In case you're wondering, fiat money is also an experiment.
145
875
3.7K
Show this thread

2.1 Bitcoin é pirâmide? Bitcoin é ilegal?

No Brasil, a propriedade e uso do bitcoin são legais e regulados por normas infralegais como a IN nº 1.888 da Receita Federal. Há países que criminalizam e reprimem sua mineração, como a ditadura totalitária da Venezuela[195].

Há dezenas de bandidos que usam o bitcoin, do mesmo modo que há incontáveis esquemas ilegais que usam reais, dólares, euros e toda espécie de ativo.

Não se pode confundir a moeda ser criminosa com a moeda ser usada por criminosos. De fato, o crime usualmente adota tecnologias mais rápido que outros setores. Há registros públicos e notórios de mais e mais atividades criminosas utilizando bitcoins. Inicialmente eram os estelionatários, agora também usam os sequestradores[196] e os "empresários" ligados ao MBL[197].

A lei brasileira não define o que é pirâmide, embora desde 1951 (Lei 1.521/51, art. 2, IX) puna até mesmo a participação em "pichardismo", "bola de neve" e "quaisquer outros equivalentes", como se existisse analogia em tipificação criminal.

Segundo a justificativa da lei, Manuel Severo Pichardo[198] fazia o mesmo esquema que Charles Ponzi fazia nos EUA: ambos ofereciam retornos acima do mercado sem ter qualquer produto, pagando os antigos investidores com a grana dos novos. No primeiro dia que saírem mais recursos que entrarem, os operadores do esquema sumirão (*exit scam*), quebrando com o lucro concentrado no topo e o prejuízo na base, por isso a metáfora da pirâmide.

Nessa definição, o INSS seria um grande exemplo de pirâmide (ainda mais imoral por ser obrigatório). Restaria inviável se não fosse a faculdade de o governo imprimir sua moeda soberana o quanto quiser, diluindo o valor das vítimas que a acumularam. Isso sem contar que a fecundidade e os índices de contribuintes previdenciários só fazem cair. O passivo aumenta e os ingressos diminuem sistematicamente, garantindo o calote branco.

O Bitcoin não é uma empresa, não tem um responsável, ninguém promete retorno algum e o ecossistema passa meses liberando mais grana do que entra no mercado sem deixar de operar e ter liquidez (na verdade, o bitcoin passou 2x mais tempo em baixa que em alta).

Além disso, o bitcoin é um ativo que tem valor derivado da sua utilidade e não de qualquer promessa, devido às suas propriedades intrínsecas (fungibilidade, durabilidade, divisibilidade, portabilidade e escassez). Por isso, não satisfaz nenhum dos três critérios de “pirâmide”.

É provável que sua aposentadoria, herança, cargo, renda ou concessão públicas não existam ou não tenham valor significativo em 25 ou 35 anos, devido a questões estruturais (disrupção tecnológica com evolução exponencial) e questões políticas (colapso dos Estados Sociais com proliferação de paraísos regulatórios e fiscais e ditaduras totalitárias sem precedentes). É melhor para quem é credor (presente ou eventual) do Estado (nem que seja de expectativa de direito) ter 5-10% do patrimônio em bitcoin ou arriscar a perda total apostando tudo na solvência futura e eventual de devedor que já é insolvente?

Talvez o Bitcoin não exista mais em 20 anos, mas, se ele existir, servirá de *hedge* devido às suas características idiossincráticas e à baixa correlação com ativos convencionais (que justificam a tese[199] de "nova classe de ativo").

2.2 Qual é o lastro do Bitcoin?

O *Gold Standard* deu errado todas as vezes em que foi tentado, até o choque de Nixon em 1971 e o fim do acordo de Bretton Woods[200]. Em todas as vezes que algum governo ou banco emitiu, por tempo ou volume significativos, moeda escritural ou *IOU* (I owe you) supostamente conversível em ouro, houve calote, formal ou branco. Esta é a razão de o Bitcoin ter sido criado: sistemas baseados em confiança falharam sistematicamente por milênios.

Lastro como garantia de escassez é o *software* que limita sua emissão e seu sistema de governança para que cada nó siga a regra que quiser. Se eventualmente usuários decidirem que a emissão de bitcoins vai aumentar (ou quiserem mudar qualquer outra regra), aqueles que não concordarem podem continuar rodando seus nós com as regras originais, gerando um *fork* (divisão da rede, como ocorreu mais de uma dezena de vezes como o *bitcoin cash* e o *bitcoin gold*). Até hoje, todos os *forks* deram prejuízos aos dissidentes e lucro aos *holders* que desovaram as "moedas grátis" nas primeiras horas em que eram listadas.

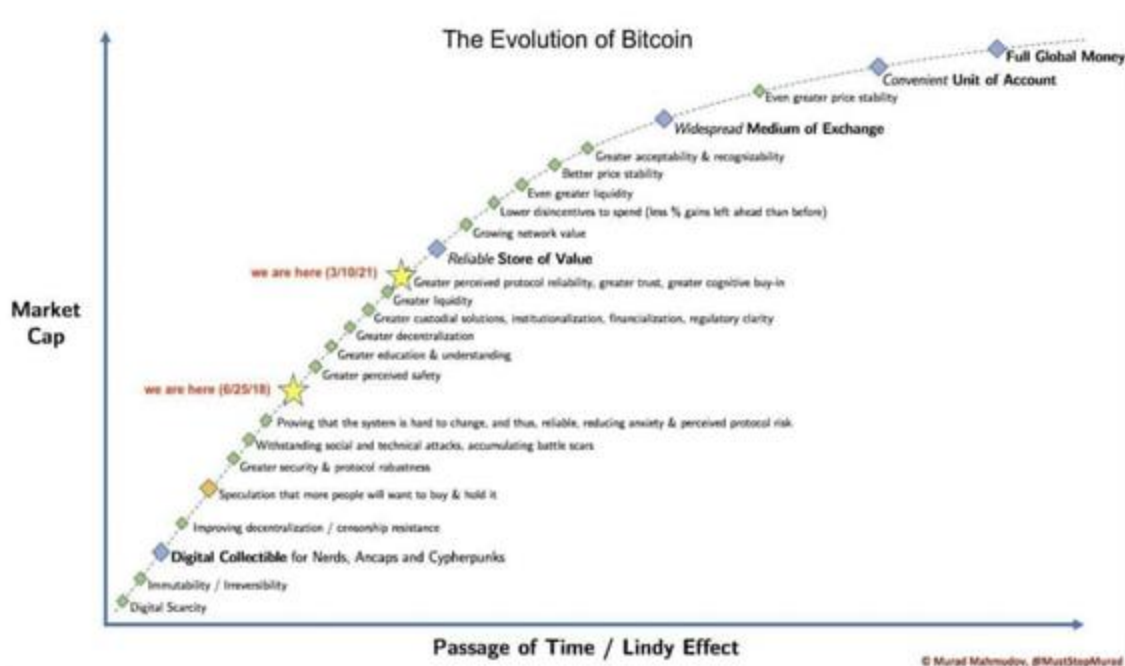
Lastro como valor-utilidade é derivado das suas funções (reserva de valor imune a expropriação, transações, controles de capitais e sistema de registro e comunicações incensuráveis) e é diretamente proporcional a abusos estatais em tabelamento de preços, censura, expurgos, diluição da moeda, controles de capitais e *déficits* em orçamentos públicos. Por isso, acredita-se que, se o *gold standard* fosse respeitado, o Bitcoin nunca existiria.

Lastro como conversibilidade é a possibilidade de usar o *token* para fazer transações e registros públicos (graças aos bilhões em investimento irrecuperáveis em *ASICs* dos mineradores, profissionais comprometidos, empresas do ecossistema e toda infraestrutura).

As moedas fiduciárias não têm lastro de conversibilidade (quando não estão em regime de paridade com outra *fiat* ou com emissão limitada por *currency board*) e não têm lastro como garantia de escassez, só tendo algum valor porque os tributos têm que ser pagos em *fiat* e devido ao curso

forçado (*legal tender*) – a obrigação legal de as vítimas aceitarem a moeda como pagamento ou sofrerem violência.

2.3 Bitcoin vai substituir as moedas estatais?

Como ilustrado na figura “tendências de adoção”, existe uma série de passos para um ativo se tornar moeda mundial plena:

A tendência, seguindo o caminho dos ativos já usados como moeda, seria substituir, primeiro, parte do mercado do ouro; depois, paraísos fiscais e *offshores*; então, imóveis, ações e títulos como reserva de valor.

Os ativos que seguiram essa progressão evoluíram por séculos. Não sabemos se, no nosso tempo de vida, o bitcoin substituirá as moedas nacionais.

Se alguns governos fizerem reservas em bitcoin, nem que seja através de expropriação, desapropriação ou tributação, talvez algumas moedas nacionais sejam lastreadas em bitcoin e durem mais uma ou duas gerações.

Em um de seus interessantes *insights*, Robert Breedlove deixa claro como moedas que funcionam como reserva de valor modificam o comportamento dominante de seus usuários: o dinheiro capitalista do livre mercado (bitcoin e ouro) incentiva a economia, já que a escassez gera apreciação e atenua as distorções do mercado, assim moralizando-o; já a moeda socialista (moeda fiduciária) incentiva o endividamento, à medida que a inflação diminui os

encargos das dívidas reais. Por esse motivo, existe a tese de que o uso generalizado do Bitcoin provocará uma Revolução[201] ou Renascimento[202] moral, tecnológico e material.

Mircea Popescu[203], desde 2012, advoga o oposto: que Bitcoin é a coisa mais conservadora neste planeta desde Jesus — vez que vai restaurar Lei Natural, moralidade, propriedade, liberdade e instituições naturais, como expresso no meme “BITCOIN FIXES THIS". Cristo mudou o mundo, mas afirmou que não vinha mudar a Lei (Antigo Testamento), mas sim para fazê-la ser cumprida[204].

2.4 A computação quântica não destrói o Bitcoin? O Bitcoin não foi hackeado?

Não, o Bitcoin não foi hackeado, empresas que usam o bitcoin sim**.**

Computadores quânticos[205] são computadores que exploram a mecânica quântica para realizar certos cálculos muito mais rápido que os computadores tradicionais.

Na computação quântica, os algoritmos e *softwares* processam informações através de sistemas quânticos, como átomos, fótons ou partículas subatômicas. Computador quântico não é uma máquina que roda mais rápido as mesmas aplicações, ele apenas é um artefato capaz de "rodar" alguns algoritmos específicos.

Um computador quântico suficientemente potente causaria alguns problemas ao Bitcoin. Porém, cabe salientar que a computação quântica não é uma ameaça só ao sistema de criptografia do Bitcoin, mas a todos os sistemas computacionais no mundo que utilizam aparatos de criptografia semelhantes com criptografia de chave pública-privada derivada de curva elíptica: sistemas bancários e de autorização de disparos de armas atômicas, por exemplo, seriam alvos em muitos aspectos mais vulneráveis e lucrativos. Outro *honeypot* preferencial seriam as carteiras antigas de Satoshi Nakamoto (ainda em tecnologia mais vulnerável).

Um endereço de Bitcoin está protegido de computação quântica desde que nunca tenha sido gasto. Ou seja, nunca tenha sido revelada a chave pública, por isso, usar cada endereço apenas uma vez é considerado procedimento padrão. Um endereço é o *hash* de uma chave pública. A chave em si só é revelada quando há gasto daquele endereço (e não depósito).

No entanto, ainda há tempo para a mudança de todo o cenário da área de segurança criptográfica de chaves públicas, com o desenvolvimento dos protocolos de criptografias quânticas. Há algumas pesquisas acadêmicas em andamento sobre a criação de algoritmos de chave pública com segurança quântica com muitas das mesmas propriedades dos algoritmos de chave pública de hoje, mas isso é muito experimental.

Computadores quânticos funcionais podem levar algum tempo (algumas gerações), principalmente porque é provável que os primeiros computadores quânticos sejam extremamente lentos, mas práticos para realizações de projetos específicos. Os computadores convencionais são ainda muito

rápidos em diversas atividades de processamento de informações e podem realizar muitas ordens de magnitude a mais por segundo, porque vêm sendo aprimorados nos últimos 40 anos.

O ex-desenvolvedor do *Bitcoin Core* Peter Todd[206] esclarece que o computador quântico não pode resolver qualquer tipo de problema com tanta velocidade de processamento; mas consegue resolver problemas específicos com uma grande rapidez, pois foi projetado para realizar um tipo de função de forma específica.

Atacar chaves criptográficas do Bitcoin exigiria cerca de 1.500 *qubits*. Atualmente, o mundo não possui a tecnologia necessária para criar um computador quântico grande o suficiente para atacar a criptografia da rede Bitcoin[207]. Não se sabe com qual rapidez essa tecnologia avançará, o ECRYPT II[208] estima que as chaves *ECDSA (Elliptic Curve Digital Signature Algorithm)* de 256 bits do Bitcoin tendem a ser seguras até, pelo menos, 2030-2040.

O Bitcoin já possui alguma resistência quântica embutida que proporciona uma mitigação necessária. Se você usar apenas endereços Bitcoin uma vez, o que sempre foi a prática recomendada, sua chave pública *ECDSA* só será revelada quando você gastar bitcoins enviados para cada endereço.

Um computador quântico precisaria ser capaz de quebrar sua chave no curto espaço de tempo entre o momento em que sua transação é enviada pela primeira vez e quando ela entra em um bloco. Entretanto, precisar-se-iam de décadas para que um computador quântico quebrasse uma chave criptográfica de Bitcoin, que, com as melhores práticas, só ficaria vulnerável por minutos.

Em outras palavras, segundo os *experts*, os medos sobre a computação quântica são exagerados e, apesar dos avanços nesta área, os engenheiros e cientistas ainda não sabem como criar um computador quântico suficientemente complexo a ponto de *hackear* o Bitcoin. Além disso, no dia em que essa missão for cumprida, deve ser adotado novo esquema criptográfico; e, antes de as carteiras mais recentes serem atacadas, as carteiras antigas e demais *honey pots* servirão de "canário na mina[209]".

Por fim, é útil lembrar que a ameaça da computação quântica já está sendo enfrentada com o desenvolvimento de provas de trabalho *quantum resistants.* Quando surgir uma máquina capaz de quebrar o *Proof of Work* da

Blockchain, basta aplicar rapidamente um *fork* para mudar essa prova de trabalho.

Em suma, computação quântica: a) está tão próxima quanto fusão nuclear (ou seja, possível em laboratório ou simulações, mas pode levar décadas ou gerações para aplicações comerciais); b) afetaria mais bancos e sistemas de defesa e infraestrutura (por serem maiores *honeypots* e mais vulneráveis) que o Bitcoin, "não preciso correr mais que o leão, preciso correr mais que você"; c) afetaria primeiro o milhão de bitcoins atribuídos a Satoshi em endereços antigos (e milhares de BTCs em endereços usados) e eles não ligam, temos canários na mina; e, d) poderia deixar de ser uma ameaça ao Bitcoin com atualização, já que é um software.

2.5 Quando eu morrer, para onde irão meus bitcoins?

Um caso seminal de como preocupações sucessórias com bitcoin se tornam práticas foi o de Hal Finney[210].

Quando bitcoins são enviados para endereços que não têm chaves privadas conhecidas (ou quando as chaves privadas para acessar saldos de endereços são perdidas), essas unidades passam a estar "perdidas". São como o ouro no fundo do mar, talvez um dia haja tecnologia para recuperá-los, talvez não.

Há diversas estimativas forenses[211] indicando entre 2,8 e 3,8 milhões de *tokens* perdidos (inacessíveis, provavelmente para sempre), aumentando a escassez e o valor das demais unidades.

Respondendo à questão, se você morrer, os bitcoins vão para onde você quiser, algumas possibilidades básicas podem ser enumeradas:

a) podem não ir para ninguém, enriquecendo o resto da comunidade, se você não deixar informações de como recuperar suas chaves privadas e senha, como único ativo que pode levar consigo para o túmulo;

b) podem ir para seus sucessores, legalmente, como qualquer saldo bancário, se tiver depositado em plataforma com *KYC – know your customer* (como walltime.info);

c) se a chave privada estiver impressa em papel, sem estar criptografada, quem tiver a posse material do papel passará a ser o proprietário dos bitcoins;

d) se estiver impressa em *paper wallet* criptografada, os bitcoins só serão acessados por quem detiver a chave e a senha (por isso, alguns *bitcoiners* informam aos sucessores como descobrir a senha e a chave, ou dão a senha a algumas pessoas e o acesso às chaves a outras);
e) se baixaram *wallet* no celular, ao recuperar o aparelho com senha, recuperam-se os bitcoins; ou
f) se for encontrada *hardware wallet*, quem souber a senha e tiver posse do aparelho poderá acessar os bitcoins.

Ou seja, Bitcoin dá a liberdade de planejar a sua sucessão mesmo fora dos limites legais de disposição. Se o usuário não revelar a potenciais sucessores que tem bitcoins, nem deixar nenhuma forma de eles descobrirem, é porque não quer que eles fiquem com nada.

Existe um dilema *(trade-off)* entre segurança e praticidade. Quanto mais acessíveis os bitcoins, menos seguros. Por isso, são mais confiáveis plataformas que mantêm quantidades maiores de saldos *off-line* (*cold wallet*) e menos *on-line* (*hot wallet*), sem contar os meios de aumentar segurança com *timelock* (saldos bloqueados por certo tempo) e *multisig* (exigência de múltiplas assinaturas para movimentação).

Exemplos extremos são o de quem concreta partes da *seed (mnemônicos)* em imóveis diferentes – exigindo tempo e acesso a ambos os imóveis para acessar os bitcoins; ou de quem concreta a *seed* (3 a 24 palavras, usualmente) criptografada em sua casa, informando pessoas de sua confiança que não têm acesso à *seed* a senha para descriptografar tal sequência.

Esquemas de *multisig* que exigem 4 ou 5 assinaturas de um total de 7 são usuais e permitem à família ou à sociedade empresarial continuar tendo controle dos bitcoins por maioria, mesmo com morte ou dissidência simultânea de 2 ou 3 atores (embora contenha risco no cenário de morte simultânea da maioria das partes, o que também pode ser mitigado pelo *backup* físico de suas chaves, nem que seja em cofre ou concretado em sua casa).

Uma simplificação da solução *multisig* é o *"Shamir's Secret Sharing scheme"*, disponível até mesmo em hardware *wallets* mais modernas.

Shamir Scheme permite que a maioria das pessoas que possuem partes da senha acessem o total dos saldos, sejam conjuntos de 2 de 3, 3 de 5 ou 4 de

7.

Assim, se você der uma senha dessas a sua mãe, uma a sua esposa e uma a seu testamenteiro, seriam necessários 2 desses 3 para sacar o saldo — não havendo perda mesmo com mortes simultâneas sua e de mais um deles.

Segregar diferentes *passphrases*[212] para saldos que queira deixar para cada sucessores é uma alternativa mais segura quanto a oportunismo, porém com mais risco de bitcoins serem perdidos em caso de mortes simultâneas. As palavras (*seed*) poderiam estar em local conhecido por todos os sucessores — em cofre ou concretada — e a respectiva *passphrase* seria entregue a cada um deles – o que pode ocorrer até após sua morte, automaticamente por *e-mail*.

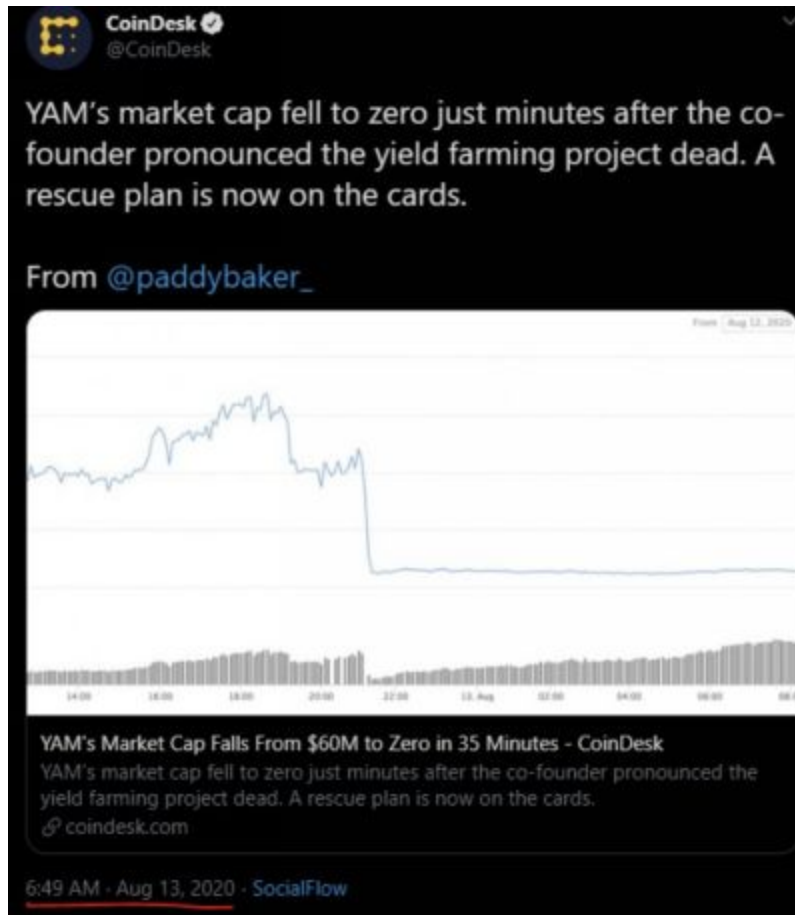
Nesse caso, a ferramenta sucessória útil é a função *"Dead man`s switch*", disponível desde 2013 gratuitamente no *Gmail* ou *“final message service”* (https://finalmessage.io/) que permite automatizar uma mensagem para alguém de sua confiança, que só é enviada após certo período de inatividade.

A mensagem final também pode ser *multisig* (multi assinaturas), forçando consenso entre sucessores para saque (total ou parcial). Há solução semelhante na rede *Lightning Network*[213].

Em resumo, ativando essa opção, são enviadas automaticamente mensagens por *e-mail* quando a conta atingir certo tempo de inatividade. Desta maneira, pode expressar suas últimas vontades, dando as instruções a seus sucessores de como acessar seus ativos — informando senhas e saldos (ou onde encontra-los) apenas para os beneficiários, sejam herdeiros ou legatários.

É vital lembrar que pode ser disparado antes de sua morte — caso fique a deriva, preso, hospitalizado, em cativeiro ou por qualquer outro motivo sem acesso à conta.

Até o desenvolvimento do Bitcoin não existia bem que não pudesse ser tomado à força, nem ativo cujo titular pudesse garantir que não fosse adquirido por ninguém após sua morte. Por isso, as nuvens mudaram o jogo, a criptografia é uma arma de guerra desde sua criação. Seu uso, nesse caso, inviabiliza a vitória por pura violência e força bruta.

2.6 Era vantagem comprar no início, não agora! Não seria melhor comprar a *shitcoin* que custa apenas 1 satoshi em vez de bitcoin? Ou comprar uma NFT que pode valer milhões em algumas semanas?

O valor de ativos que geram fluxos de caixa é calculado pelo fluxo de caixa esperado descontado pelos riscos e pela taxa de juro de mercado. O valor de *commodities* é normalmente correlacionado a sua escassez, como previsto no modelo do *stock to flow*[214].

Por isso, pretender ganhar mais comprando *altcoin* que bitcoin é o mesmo que pretender ganhar mais comprando cobre, alumínio ou ferro do que ouro. É possível aumentar seu patrimônio em ouro fazendo *trades* com prata, mas, no longo prazo, ao longo dos últimos 3.000 anos, quem manteve posições em prata por gerações seguidas invariavelmente perdeu poder de compra, medido em ouro[215].

A chance de uma *altcoin* substituir o bitcoin é a mesma de outro metal substituir o ouro.

A prata na Idade do Bronze valia 1/6 do grama do ouro, em Roma 1/12, nos padrões bimetálicos 1/16 e, desde a década de 1980, varia entre 1/35 e 1/125. Realmente, uma curva de baixa de mais de 3.000 anos. Estimativas de abundância de prata e ouro variam entre 1:16 e 1:18 (na crosta terrestre), entretanto, as relações de valor e escassez marginais não são lineares, mas exponenciais.

Uma comparação semelhante pode ser feita observando o índice de "dominância" do bitcoin (excluindo *stable coins* e *scams* com volumes e cotações manipuladas).

Altcoins são exponencialmente mais arriscadas que bitcoin e a maioria delas "virou pó" ou tende a virar após os controladores venderem o suficiente de suas posições.

Entre maximalistas, é crescente o entendimento que *altcoins* eram necessárias no início como *test nets (redes para testes de inovações) ou* camadas alternativas para envio de valores quando *fees* estivessem altas, porém, com soluções *offchain*, 2ª camada e *sidechains*, essa demanda não existiria mais e as *altcoins* seriam hoje apenas ataques de engenharia social contra o bitcoin (ou, mais especificamente, contra detentores de BTC sem estrutura para mantê-los). A única função intacta das *altcoins* é a de redundância, de manter sistemas ativos caso o Bitcoin pare de funcionar, por qualquer motivo e para testar conceitos em redes de menor valor.

De fato, há muitos fatos fundamentando alegações de que criadores em série de dezenas de *shitcoins* acumulam bilhões de dólares em *assets* sem investir nada além de promessas.

Evidências de golpes na criação de novas moedas são: adoção de *Proof of Stake* — esquema para remunerar quem já possui saldos; subsídio para desenvolvimento (vinculação de novas moedas para projetos que seriam aprovados por maioria, que são os próprios fundadores); e, *pre-mine*, ou seja remuneração em milhares de *tokens* pela "ideia" de criar a moeda[216].[217]

Grande parte das pessoas que ganham na loteria terminam piores do que se não tivessem ganhado. Perdem sua família, emprego, desperdiçam o prêmio e, no final, terminam mais pobres do que eram.[218]

Ter bitcoin é ganhar na loteria aos poucos. Só que a maioria das pessoas que obtêm grandes valorizações, por ausência de estrutura mental, emocional e familiar, perde tudo – seja com meretrizes, cocaína e luxos absurdos, seja vendendo tudo para recomprar mais barato depois (confirmando que, em geral, depois é nunca); ou mesmo comprando *shitcoins* para "aumentar o número de bitcoins".

A maioria das *shitcoins* já viraram pó. Mais de 90% dos *forks* do bitcoin morreram, ninguém minera e nem há mercado para negociar esse *tokens*.

Esses golpes geram lucro aos seus criadores (principalmente por pré-mineração) e às corretoras (tanto em *fees* quanto cobrando para listar as *shitcoins*), invariavelmente. Alguns especuladores também lucram esperando comprar para vender "quando subir", porém, eventualmente não sobe mais e os últimos a adquirir perdem tudo. É um jogo de soma negativa, mais riqueza é perdida que produzida – e a maioria absoluta dessa riqueza é capturada pelos golpistas e *exchanges* (*shitcoin casinos*), "a casa nunca perde".

Quando alguém disser que ganhou dinheiro com ether, doge, shiba ou ripple – lembre-se que muita gente também ganhou com Telexfree, BBOM, Atlas Quantum, GBB, Minerworld, Ronaldinho 18K ou em "ações memes"[219].

2.6.1 Se *shitcoins* não são alternativas? Como diversificar?

Graças a mercados futuros de bitcoin, é possível fazer *"cash and carry"* travando ganhos acima de 30% a.a. em dólar nos mercados de alta[220]. Também se pode obter renda, em dólar ou ouro, com taxas de *funding* e *lending*[221]. de *stables*. Infelizmente, não existe investimento em ambiente de juro real negativo, apenas *hedge* ou perda – fixa ou variável.[222]

Ler esse livro é diversificar: investir tempo em sua educação real. Alternativas de diversificação também são: investir em sua produtividade (em negócio próprio, em suas habilidades e *networking*) ou relações sólidas, como criar filhos dispostos e capazes de ser úteis.

Como Saylor deixa claro, quando você sabe qual a solução para um problema de engenharia, diversificar é "vender o vencedor, para comprar perdedores".

Na dúvida, pesquise no *ranking* dos bilionários quantos concentraram mais de 90% em apenas um ativo (Musk, Bezos, Gates…) e quantos diversificaram.

Seja grato:

A oportunidade de trocar "papel colorido lastreado em honestidade de político" por dinheiro de verdade logo vai acabar.

Quem veio na 1ª onda pôde ter milhares; na 2ª, centenas; na 3ª, dezenas; e na 4ª vão ser unidades ou mesmo frações.

Muita gente perdeu mais de 90% de sua riqueza investindo em *shitcoins* ou confiando em desconhecidos para fazer a custódia de suas moedas. Esteja aberto a aproveitar a oportunidade que você tem, ou a desperdiçará e lembre-se: *not your keys, not your coins*.

Sem gratidão você não recebe nada. Para receber algo de valor precisa estar aberto a aceitar. Para estar aberto precisa reconhecer o valor do que vai receber e como uma graça a oportunidade. Esse é um dos "fatores bilionários" identificados por Napoleon Hill[223].

Com *fiat*, a volatilidade é zero e há certeza de perda de poder de compra. No Bitcoin, a volatilidade é alta, perdas acima de 30% são comuns até em mercados altistas (*bull markets*) e de até 90% na baixa (*bear market*). Entretanto, seu retorno médio na década é superior a triplicar a cada ano (200% a.a.), em dólar. Prefere volatilidade ou certeza de perda?

O maior legado não é material.

As coisas mais baratas são pagas em *fiat* ou dinheiro. As coisas realmente valiosas são pagas com seu tempo de vida, honra, saúde ou oportunidade – e é de natureza moral, emocional, espiritual e educacional. Não existe almoço grátis.

Mais riqueza foi criada nos últimos 20 anos que nos 20.000 anteriores ao século XX, entretanto, se a tecnologia moderna não estiver mais disponível, 80% da população não terá como se alimentar em menos de uma semana, morrem de fome. Quanto mais complexos os sistemas, mais frágeis.

Ninguém vive de riqueza acumulada para sempre, você tem que se preocupar em transformar seus filhos em pessoas capazes de multiplicar e gerar riqueza – materiais ou não.

O comunismo é a escravidão suprema e para ser escravo é essencial que não tenha família, Deus ou legados – isso que vai acontecer se falharmos. Se você tem a Deus, família ou sabe de onde veio, não é escravizado. Como muito bem explicou Fernando Pessoa há quase 100 anos[224]:

Se o que há de lixo moral e mental em todos os cérebros pudesse ser varrido e reunido, e com ele se formar uma figura gigantesca, tal seria a figura do comunismo, inimigo supremo da liberdade e da humanidade, como o é tudo quanto dorme nos baixos instintos que se escondem em cada um de nós. O comunismo não é uma doutrina porque é uma antidoutrina, ou uma contradoutrina. Tudo quanto o homem tem conquistado, até hoje, de espiritualidade moral e mental — isto é de civilização e de cultura —, tudo isso ele inverte para formar a doutrina que não tem.

Dada a inviabilidade dos Estados Sociais e a radicalização das "bolhas", não há possibilidade de acordo: ou a humanidade será livre e próspera como ninguém nunca foi (se o totalitarismo for inviabilizado ou derrotado, com o extermínio dos criminosos pelos mercados de apostas descentralizadas de morte); ou, será escravizada e submissa de maneira sem precedentes, se o modelo chinês for dominante, com monitoramento de cada palavra (dita, ouvida ou escrita) e sistemas de crédito social[225] e expurgos[226].

Seu tesouro está onde está o seu coração. Todos os dias renunciamos um pouco de nossa liberdade, cada opção é renunciar a todas as alternativas. Dinheiro é a forma de concentrar tempo, liberdade e esforço para conseguirmos a liberdade (em tempo livre, risco e esforço) de outras pessoas.

Vender bitcoin para realizar um sonho, melhorar sua saúde, obter independência financeira ou adquirir território soberano é totalmente compreensível. Contudo, até o final desse ciclo, com as plataformas de colateralizados contra carteiras diversificadas, nem isso será necessário.

Exemplos de pioneiros que moram na mesma casa e mantêm o mesmo padrão de vida são Nick Szabo e Laszlo[227] (que 10 anos depois da pizza de 10 mil bitcoins ainda morava na mesma casa).

Há dezenas de exemplos opostos: de gente que desperdiçou a riqueza com “lambos”, *NFTs*[228] (*uma forma quase tão boa de lavar dinheiro quanto o próprio mercado de arte*[229]), drogas, prostituição e ostentação absurda ou perdeu tudo com *shitcoins*, falsos *giveaways*, outros golpes. A ostentação é um dos sinais de ganho fácil e é típica dos piramideiros: *easy come, easy go.*

Uma das formas atuais de ostentação absurda é a aquisição de *NFTs* por valores milionários. *Tokens* não fungíveis foram concebidos[230] em 2012, “*colored coins*”; e, existem exemplos desde 2014. Podem ser úteis como prova pública de certificado de autenticidade ou propriedade.

Se um artista ou casa de leilão envia *NFT* comprovando que detentor de certo endereço é o comprador legitimo da obra X, ele poderia transferir publicamente essa propriedade sem revelar quem adquiriu abertamente (apenas seu endereço). São análogos a *NFTs*, os elementos de jogos (personagens, *skins* e elementos particulares ou genéricos, ou fungíveis, seriam *"drops")* em ambientes fechados centralizados. Também podem ser registrados em *sidechain,* como na *Liquid*[231].

Em suma:

a) Mais de 90% das *altcoins* são golpes e mais de 99% incapazes de entregar o que prometem. Você conhece quem está à frente do projeto? Estudou o *whitepaper*? Grande parte dos projetos são cópia da cópia do *paper* principal ou copiam melhorias propostas nos *BIPs*;

b) Existem vantagens em todas essas experiências com *altcoins*. Porém, há também choro e ranger de dentes, a cada ciclo;

c) O tempo e esforço necessários para acompanhar *shitcoins* é enormemente maior do que fazer o mesmo com o Bitcoin.

2.6.2 Melhores práticas de segurança para custódia própria de bitcoin:

Sua *OPSEC* (segurança operacional) sempre vai variar com sua tolerância a riscos e com o ambiente. A Internet não esquece nada. Uma foto de rosto pode identificar qualquer um. Perfis identificáveis em redes sociais ou mesmo registro de localização em eventos políticos podem resultar em expurgos e perseguição derivada da associação de *big tech* com governos totalitários. Dai a importância de Satoshi permanecer anônimo. Privacidade vai passar a ser mais valiosa que popularidade com o entendimento do poder do *big data.*

Para não ser vítima, leia e entenda as "seis leis de Maca para não ser roubado"[232]

Se sua *bag* for menos de 10% do seu patrimônio total, manter *hardware wallet* bem guardada com *seed (*com *passphrase)* em múltiplos imóveis (em caso de incêndio, por exemplo) ou em chapa de aço (como da *Stackbit*[233] ou *Seedplate* da *Coinkite*) em lugar seguro é, normalmente, o suficiente.

Se seu investimento em BTC for para as futuras gerações; ou, for mais de 2 ou 3 anos de sua renda; ou, mais de 50% de seu patrimônio, manter em *hardware* mais de 10% a 20% dos saldos é loucura, mesmo com *plausible deniability*[234].

Melhor prática, no caso, é deixar os *hardwares* todos resetados – até para pensar bem antes de mover e mandar para Elon Musk (em falso *giveaway*[235]); ou, pior, dar a senha sob ameaça, coação e constrangimento[236], *"Wrench attack*"[237], situação que, ganhando tempo,

pode até mesmo conseguir janela de oportunidade para matar sequestradores – já que sabe que se eles te matarem, perdem a possibilidade de acesso aos bitcoins.

Para grandes quantias, ideal é deixar de 60% a 90% em cold – pode ser *multisig* tipo *"shamir's secret sharing scheme"*, em que 3 de 5 partes têm que concordar para mover (até mandando para os parentes as palavras em arquivo criptografado por *email*); pode ser uma *paper* e uma chapa de aço (com *passphrase* e em locais diferentes). Mais simples, se não tiver um monte de herdeiros, é dar a um parente cópia das palavras e a outra pessoa (ou pessoas partes) a *passphrase*.

Por exemplo: *seed* para a mãe ou pai – e uma *passphrase* para esposa para acessar metade e uma *passphrase* para padrinho para acessar metade para dar aos filhos adultos ou aos pais se estiverem em real dificuldade. Se sua mãe achar que sua mulher te matou, ela impede perpetuamente que a cônjuge acesse os bitcoins – mas ambas podem legar as referidas chaves a netos, após a morte da outra. Se sua mãe, esposa e compadre entrarem em conluio para te roubar, realmente, bitcoin não vai ser sua maior preocupação.

Outro bom exemplo: viúvo com 5 filhos – uma *seed* no cofre ou concretada em casa em lugar que todos os 5 saibam onde está (mas que não tenham como acessar sem chamar atenção, fazer barulho e ter trabalho) e o legado de cada um é acessado com uma *passphrase* que já deu previamente a cada um deles. O máximo que cada filho poderia roubar é o saldo que já estava reservado para ele – e seria publicamente sabido.

Se você ainda quiser manter satoshis no celular para fazer pequenos pagamentos pela LN, tudo bem, só deixe a quantidade de riqueza que você sairia no bolso na rua desarmado no centro de uma cidade grande de Banânia.

Se você ainda quiser manter saldos em plataformas para fazer "*trade*", capitalizar ou gestão, pelo menos não deixe na mesma plataforma mais de 2 a 3 anos de sua renda nem 10% de seu patrimônio total – e com *whitelist* para os bandidos terem que dominar você e te manter vivo por 14 a 16 dias para poder subtrair o saldo lá.

A tendência é que os esquemas de "falsos *giveaways*", "falsas *wallets*" e "trade de *shitcoins*" sejam logo substituídos pelo *"wrench attack (trench hack)"* — alguém te dominar metendo furadeira, porrada, choque ou mutilando você e sua família para que entregue suas chaves.

Se nem você puder mover 90% a 95% dos seus BTC sem sair de casa ou esperar 14 a 18 dias, você e toda a comunidade estarão mais seguros inviabilizando esse tipo de golpe — e o parente que sair vivo ainda vai ter 10x a 20x mais grana que os bandidos para caçá-los e colocar suas cabeças a prêmio. Se a maioria fizer isso, resta inviabilizado esse tipo de crime.

2.7 Evolução das narrativas

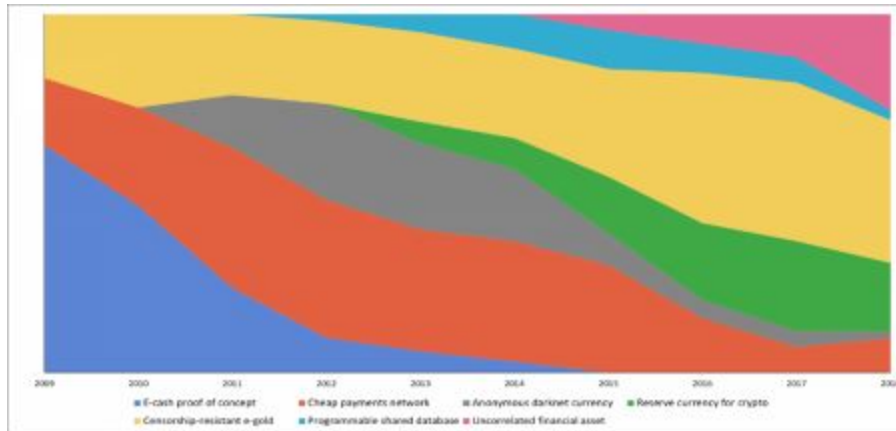
Nic Carter e Hasu mostraram em seus estudos[238] como as narrativas do Bitcoin mudaram ao longo do tempo. A discussão mais recorrente e antiga dentro da comunidade é sobre qual o principal propósito ao qual o Bitcoin deve servir: dada a sua multiplicidade de funções (meio de pagamento, reserva de valor e base de registros públicos incensuráveis) e o fato de a rede evoluir, tanto em *software* quanto em *hardware*, suas principais funções e utilidades são objeto de debate com narrativas novas a cada era.

Como se pode perceber, as visões do Bitcoin não são estáticas, logo as narrativas no universo do Bitcoin surgem, portanto, de grupos que mantêm visões muito particulares sobre o protocolo, acarretando muitas vezes “atritos” quando essas visões não são conciliáveis. Por isso, todo o aparato de consenso da rede faz com que todos os participantes contribuam para a melhor manutenção do funcionamento do protocolo.

Satoshi Nakamoto não quis ser visto como um único ponto de falha que poderia degradar bastante a segurança da rede e se ausentou em 2011. A causa provável de seu desaparecimento dos fóruns de discussões não foi explicada por Satoshi. Mas o fato de o criador se retirar não exercendo autoridade em decisões, não recebendo subsídio de desenvolvimento, nem se beneficiando financeiramente de ser pioneiro (deixando moedas paradas até hoje), é o que se denomina “concepção sem pecado”. Uma das características do Bitcoin que não há como ser facilmente repetida.

Podemos considerar que o Bitcoin ainda é um ativo em descoberta. O gráfico (*Visions of Bitcoin*)[239] a seguir mostra a influência das sete narrativas mais influentes do Bitcoin:

1. Prova de conceito de dinheiro eletrônico (azul);

2. Rede de pagamentos ponta a ponta de baixo custo (vermelha);
3. Ouro digital resistente à censura (amarela);
4. Moeda anônima da *darknet* (cinza);
5. Moeda de reserva para o ecossistema cripto (verde);
6. Banco de dados programável distribuído (azul claro);
7. Ativo financeiro descorrelacionado (rosa).

Saylor[240] defende o Bitcoin como solução de engenharia para o problema da reserva e transporte de valor - em uma argumentação muito próxima de Popescu de que "Bitcoin é pura matemática".

Em resumo, Bitcoin representa "muitas coisas para muitas pessoas": investimento especulativo; reserva de valor; meio de registro de outros ativos; meio para exercício da desobediência e desinvestimento do *legacy;* dinheiro programável; banco de dados descentralizado programável; plataforma para comunicação incensurável.

> Bitcoin is fate. It operates completely outside of any human agency, even if it was (possibly) some people that created it. For all you know about who Nakamoto was … Bitcoin might as well have created itself. The way fate works is quite simple: do the right thing and you're part of it. Do the wrong thing(s) and you're in the dark, huddling corners, wondering what went wrong and why does "the mainstream" oppress you so. And that "right thing" scarcely ever has anything to do with what "the community" thinks, wants or imagines. It is, after all, math.
>
> Mircea Popescu

3 (Why?) - Por que Bitcoin?

A necessidade vital de um dinheiro privado superior para limitar os abusos estatais foi prevista desde Rothbard e Hayek[241] em *O que o governo fez com nosso dinheiro* e *Desestatização do Dinheiro*:

> Acredito que nunca teremos um bom dinheiro novamente antes de tirar a coisa das mãos do governo, não podemos tirá-lo violentamente das mãos do governo, tudo o que podemos fazer é, por algum meio indireto, introduzir algo que eles não podem parar.

Hayek já tinha previsto que o Estado perderia o monopólio de emissão de moeda para alternativas privadas superiores. Friedman, em 1999, previu[242] objetivamente que uma "moeda digital que permita transações tão anônimas quanto as efetuadas em dinheiro" seria criada como o "dinheiro da Internet" logo que o problema do gasto duplo fosse resolvido — como Peter Thiel[243].

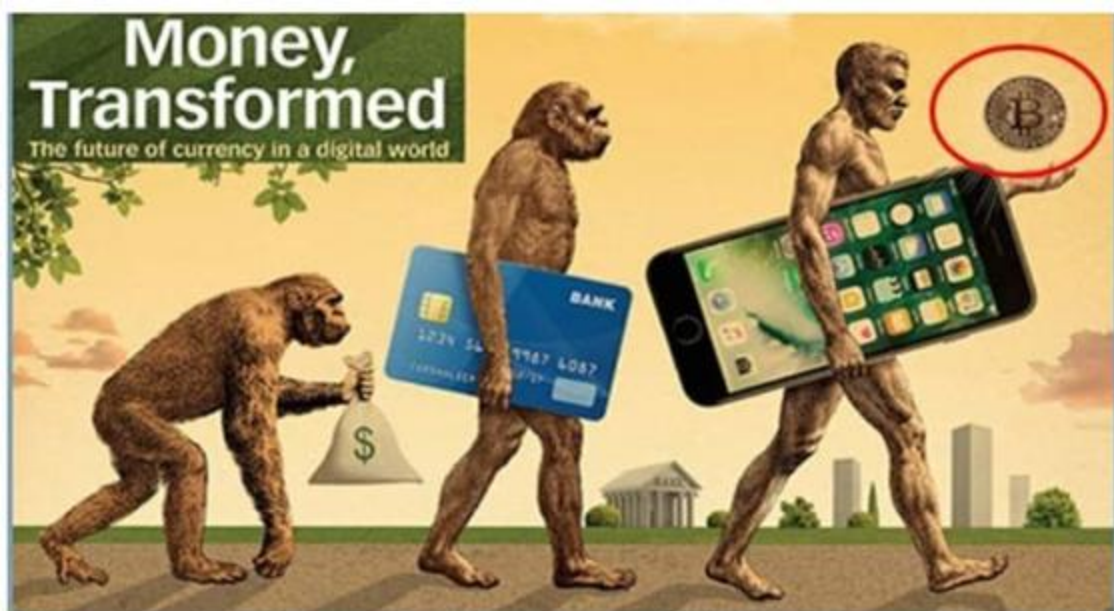
Satoshi Nakamoto resolveu o problema dos Generais Bizantinos[244] ou problema de ataque coordenado, por meio do desenvolvimento da primeira *Blockchain* viável (embora a expressão original tenha sido *timechain* em 2008).

O Bitcoin foi criado e obteve sucesso porque responde a uma demanda urgente da atualidade: um dinheiro imune a controle de capitais, expropriações e tributos involuntários, diluição por governos, e que é descentralizado, incensurável e programável.

Como Satoshi deixa claro em sua primeira mensagem no Bloco Gênese, foi o abuso do poder dos governos que os fez perder o monopólio de emissão das moedas – cada vez mais claro com a guerra ao dinheiro, os juros negativos e os *QE4ever* (alívios quantitativos perpétuos).

Satoshi Nakamoto, em seu artigo referência, reconhece as contribuições de autores e tentativas anteriores de criptomoedas e sistemas descentralizados[245] (*HashCash*, de Adam Back, e *B-Money*, de Wei Dai).

O Bitcoin não foi a primeira criptomoeda nem a primeira tentativa de sistema de pagamentos eletrônicos descentralizados, porém, foi a primeira a ter sucesso por conjugar soluções criadas até então, aprendendo com os erros das tentativas anteriores. Foi a solução necessária no momento certo.

O futuro da moeda em uma palavra: digital[246]

Linha cronológica dos predecessores do Bitcoin

ANO	SERVIÇOS/TECNOLOGIAS
1983	*eCash*
1993	*Hawthorne Exchange*
1994	*Magic Money*

1995	*Digicash/Cyberbucks*
1996	*e-gold*
1998	*BitGold*
2001	*Liberty Reserve*
2008	*Bitcoin*

3.1 Uma breve história monetária

O porquê do Bitcoin é a História da moeda[247]: a falência de todos os sistemas monetários já tentados, sejam *fiat* ou *gold standard,* falhos em honrar promessas e manter valor no longo prazo, por motivações oportunistas intrínsecas.

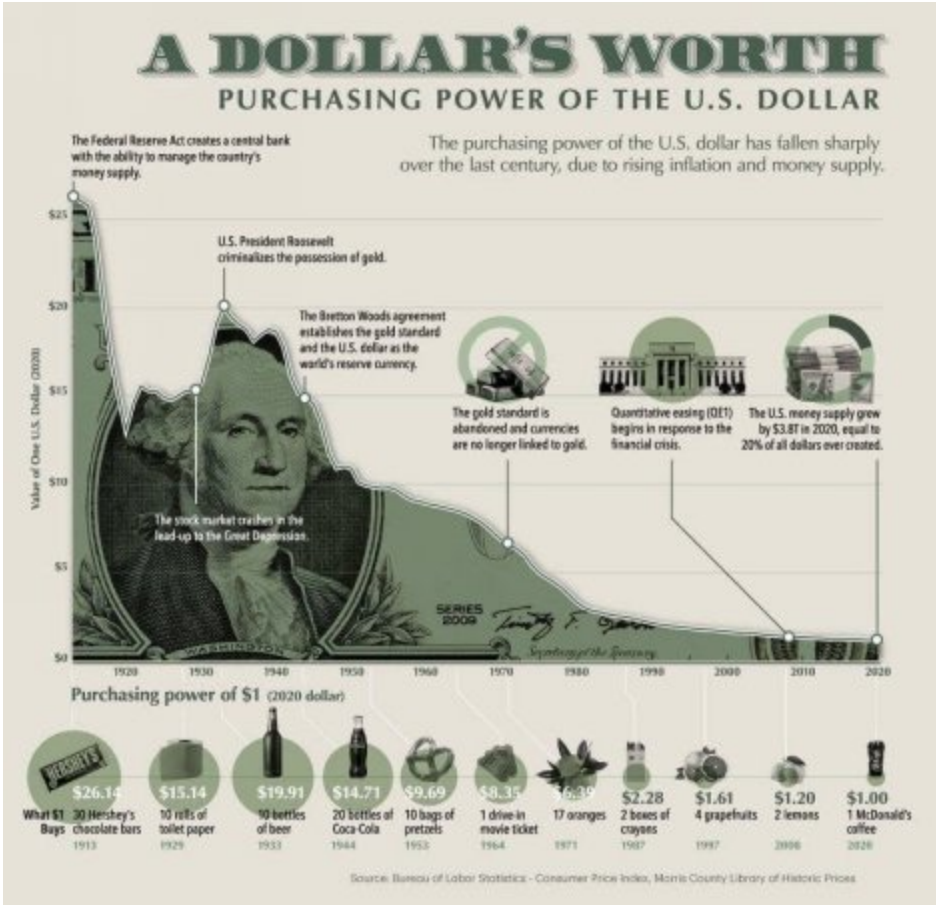
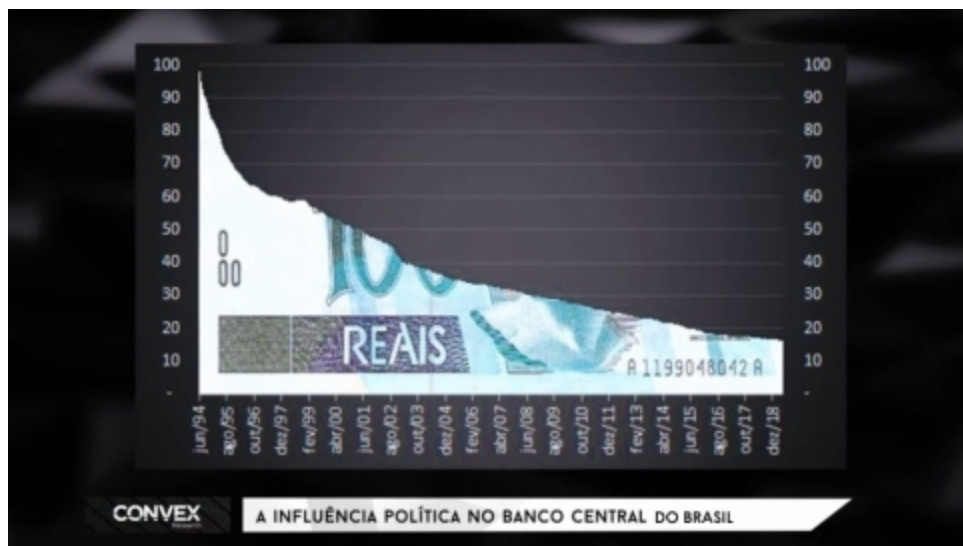
A moeda é adotada, mesmo em sistemas falhos, porque soluciona o problema da dupla coincidência de desejos[248] entre pessoas que desejam trocar entre si suas posses. Riqueza é subjetiva e criada do trabalho ou comércio[249]. Então, é possível que todos estejam em melhor condição meramente redistribuindo bens para os entes que os valorizem mais. Assim, há mais trocas quando existe moeda em vez de mera permuta direta de bens (que podem não ser divisíveis, duráveis nem transportáveis).

O fim do Acordo de Bretton Woods, em 1971, ou seja, o abandono do padrão ouro (*gold window*) tornou quase todas as moedas do mundo totalmente fiduciárias *(fiat money).*

Uma vez que os governos puderam imprimir moeda de maneira ilimitada, a moralidade política entrou em decomposição, tanto na distribuição do *welfare*[250] quanto na ampliação brutal de poderes dos governos, como no *warfare* (estatização da guerra).

Os resultados desses processos são mais guerras, mais gastos fora das capacidades arrecadatórias diretas dos governos e mais corrupção — uma vez que motivações oportunistas e consumistas a entes privados passam a ser dominantes: dos beneficiários de *welfare* que desistem de trabalhar até os bilionários que se dedicam apenas à captura administrativa[251]. Do indigente ao bilionário só vale a pena o oportunismo.

Prova disso é que os maiores bilionários do mundo são cantilionários (metacapitalistas), pessoas que gozam o privilégio de receber as novas moedas primeiro, por ter comprado influência em governos, por meio de financiamento estatal, sejam subsídios, contratos públicos ou mesmo compra dos títulos de suas empresas em *bailouts* (como denunciado no bloco gênese).

Declínio do Poder de Compra do Dólar *versus* Real

Em 1933[252], a moeda de 20 dólares (USD ou US$) era feita de uma onça de ouro (XAU); em 2020, 1 XAU chegou a custar mais de 2000 USD. Quem guardou dólar no colchão perdeu mais de 99% (em ouro) em menos de 90 anos – essa é a demonstração da senhoriagem e expropriação por inflação em um país “modelo”.

De 1839 a 1933, havia moedas circulando com 33 gramas (mais de 90% de ouro) com valor nominal de 20 USD. Em 1933, o governo desapropriou o ouro privado pagando 20 USD e logo depois tabelando em 35 USD/OZ. Relação de escassez e valor é inexorável:

BTC > XAU >> XAG >> USD >> BRL >>ARS >> VES

Agora é a vez de mostrar como a República no Brasil[253] era desmoralizada desde o início: 2000 réis de 1912 com 20g (90% prata) era equivalente a 18 gramas de prata; e 2000 réis de 1924 com 8g (50% prata) era equivalente a 4g (4/18 = 1/4.5). Em 12 anos, os réis foram diluídos em quase 5x — isso porque ainda existia lastro em metal.

Atualmente, a diluição é ainda maior e os juros negativos destroem qualquer patrimônio do poupador honesto no *legacy*. Se você tem investimento em bolsa bolivariana, como a B3, pergunte a si mesmo: quantas empresas abertas existiam em Banânia (ou outro Estado de Exceção bolivariano) em 1924? E em 1984? E, entre essas, quantas não viraram pó?

A diluição do valor da moeda leva à diluição da moral, pública e privada: menos motivação para trabalho, esforço, poupança, investimento e

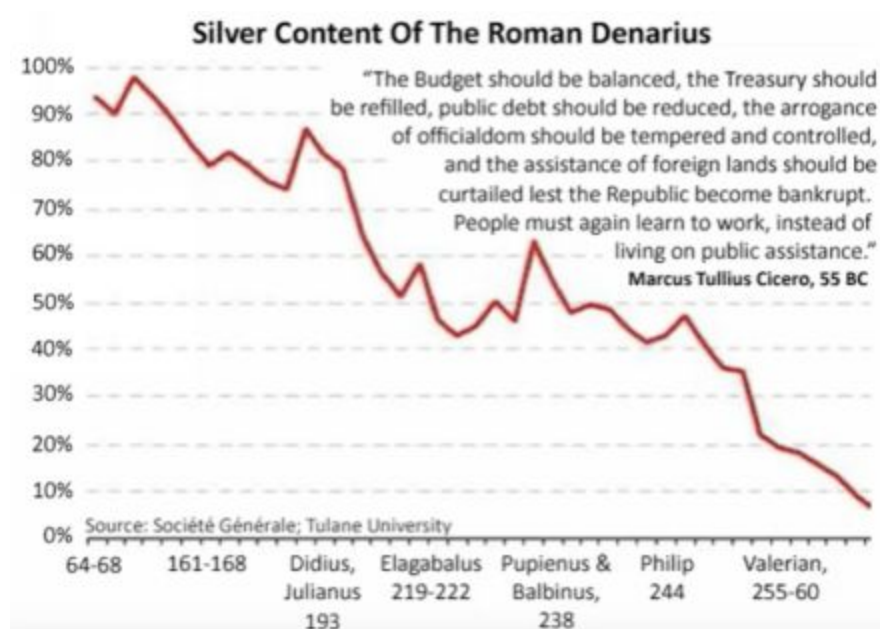
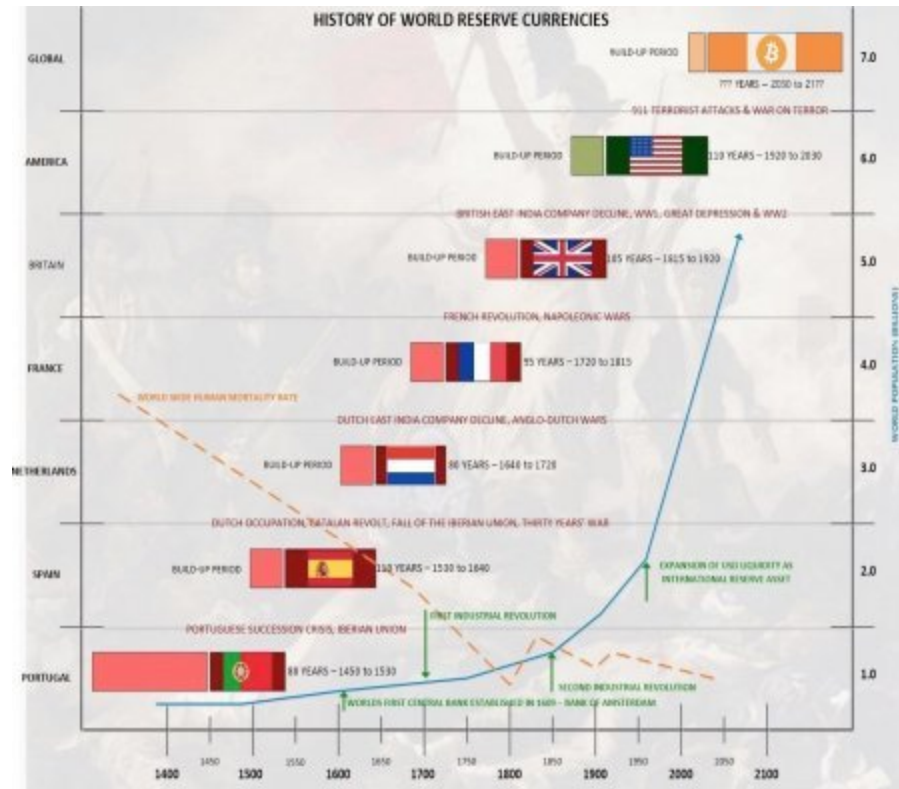
cooperação e mais motivação para vagabundagem, consumo, parasitagem, vitimismo e oportunismo.

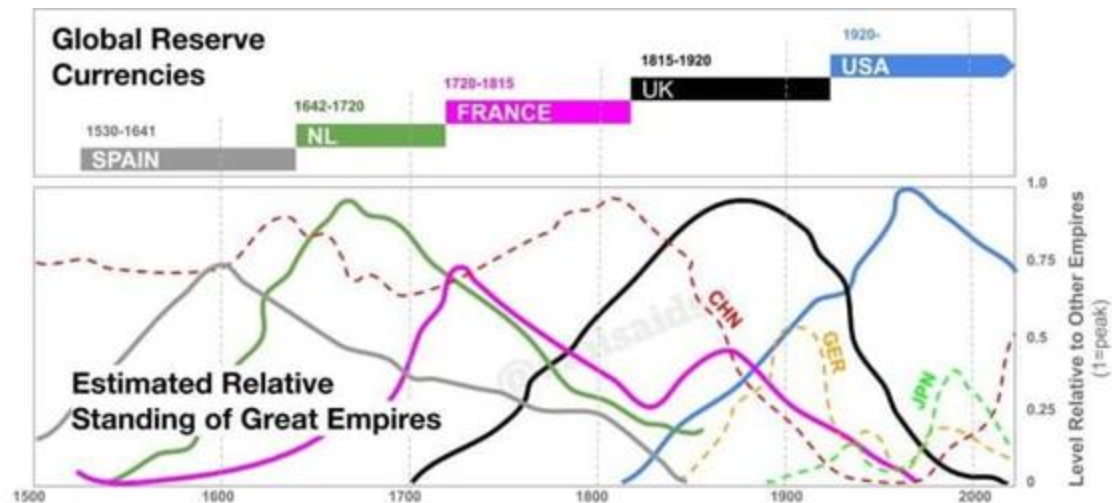
Por isso, se o Bitcoin sobreviver mais 10 anos, haverá um Renascimento moral, material e tecnológico.

O ápice das distorções veio, a partir da crise do *subprime* nos EUA em 2008, com as políticas de alívios quantitativos (QE, *quantitative easing*, eufemismo para "criar dinheiro do nada" em quantidades sem precedentes*)*, que impuseram tabelamento no preço mais importante na sociedade: o juro, preço da moeda.

Em vez de permitir que empresas em crise quebrassem, para que a inovação, o empreendedorismo e a destruição criativa atuassem como expurgo natural, os governos usaram (e continuam usando) quantidades brutais de dinheiro público para salvar bancos e empresas.

Essa atuação aumenta a desigualdade social (ao inflar o valor dos ativos), reduz o crescimento econômico (ao reduzir as motivações para poupança e trabalho) e produz as distorções que inviabilizam a continuidade dos Estados Sociais – como previsto em *O caminho da servidão*, de Hayek, desde 1944.

Como diversas civilizações, os romanos também destruíram seu império degradando sua moeda:

Domínio das moedas de reserva mundial[254]

Visualizing Interest Rates Throughout History
Dutch Perpetual Bonds
The oldest perpetual bond still generating payments is dated 1624.
Genoa Republic
4-5yr Lending Rate
1555, 1566
9.0%
1.1%
1619
U.K. 3%
Perpetual Bond
U.S. 10-year
Treasury
14.2%
1974
13.9%
1981
2.2%
1897
1.9%
1941
Financial Crisis
Eurozone Crisis
Financial crises have driven interest rates to just above zero in order to spur spending and investment.
Race to the Bottom?
Since the 1980s, interest rates set by government debt have been rapidly declining, while the global economy has rapidly expanded.
Federal Funds
Official Target Rate
Bank of England
Base Lending Rate
Sources: Sidney Homer and Richard Sylla - A History of Interest Rates, Federal Reserve, Bank of England

Dados de 500 anos das moedas de reserva global –
Posição relativa dos grandes impérios[255]

Os subsequentes *QE*s buscaram estimular a economia baixando os juros artificialmente, emitindo moeda do nada *(out of thin air*) para que os Bancos Centrais comprassem títulos soberanos (do próprio governo) e até mesmo ativos privados de qualidade no mínimo questionável, tendo atuado como investidores de última instância. Atualmente, 70% dos *ETFs* (fundos de índices, que compram ações e títulos) no Japão pertencem a entes públicos[256], e o BC Suíço[257] é um dos principais acionistas da *Exxon*, *Microsoft*, *Google*, *Facebook* e *Apple*.

O desempenho desse papel extremamente atípico por parte dos Bancos Centrais explode as suas bases monetárias e endividamento, comprometendo sua idoneidade regulatória (BCs são "donos" das entidades a que pretendem fiscalizar) e distorcendo motivações, ao superestimular a ociosidade e o consumismo e ao reprimir a poupança e a produção orientada às reais necessidades do mercado.

Diversas empresas nunca apresentaram lucros por mais de uma década, como *Amazon, Netflix* e *Uber* – sem contar as obras faraônicas e sem qualquer cabimento financeiro do "milagre chinês" (metade do crescimento do mundo desde 2008 ocorreu na China, onde abundam dezenas de milhões de residências vazias e milhares de obras[258] e empresas zumbis). Tudo isso só existiu graças a essas distorções decorrentes do juro negativo e dos "alívios quantitativos".

Observe, nesta tabela de agosto de 2021, que as taxas de juros nominais tabeladas pelos Bancos Centrais, após o ajuste dos índices de inflação de preços ao consumidor (assumindo que são idôneos), resultam em taxas negativas e, quando positivas, situam-se muito próximas do zero:

Global Central Bank Policy Rates

Country	Rate	Central Bank Rate (Today)	CPI YoY	Real Central Bank Rate	Last Move	Last Move Date
Switzerland	Target Rate	-0.75%	0.7%	-1.5%	Cut	Jan-15
Denmark	Deposit Rate	-0.60%	1.7%	-2.3%	Hike	Mar-20
Eurozone	Deposit Rate	-0.50%	2.2%	-2.7%	Cut	Sep-19
Japan	Policy Rate Bal	-0.10%	0.2%	-0.3%	Cut	Jan-16
Norway	Deposit Rate	0.00%	2.9%	-2.9%	Cut	May-20
Sweden	Repo Rate	0.00%	1.3%	-1.3%	Hike	Dec-19
Poland	Repo Rate	0.10%	4.4%	-4.3%	Cut	May-20
UK	Bank Rate	0.10%	2.5%	-2.4%	Cut	Mar-20
Australia	Cash Rate	0.10%	3.8%	-3.7%	Cut	Nov-20
US	Fed Funds	0.13%	5.4%	-5.3%	Cut	Mar-20
Canada	Overnight	0.25%	3.1%	-2.9%	Cut	Mar-20
Peru	Policy Rate	0.25%	3.8%	-3.6%	Cut	Apr-20
New Zealand	Cash Rate	0.25%	3.3%	-3.1%	Cut	Mar-20
South Korea	Repo Rate	0.50%	2.6%	-2.1%	Cut	May-20
Thailand	Policy Rate	0.50%	0.5%	0.1%	Cut	May-20
Czech Republic	Repo Rate	0.75%	2.8%	-2.1%	Hike	Aug-21
Chile	Base Rate	0.75%	3.8%	-3.1%	Hike	Jul-21
Hong Kong	Base Rate	0.86%	0.7%	0.2%	Cut	Mar-20
Saudi Arabia	Reverse Repo	1.00%	6.2%	-5.2%	Cut	Mar-20
Taiwan	Discount Rate	1.13%	2.0%	-0.8%	Cut	Mar-20
Malaysia	Policy Rate	1.75%	3.4%	-1.7%	Cut	Jul-20
Colombia	Repo Rate	1.75%	3.6%	-1.9%	Cut	Sep-20
Philippines	Key Policy Rate	2.00%	4.0%	-2.0%	Cut	Nov-20
South Africa	Repo Rate	3.50%	4.9%	-1.4%	Cut	Jul-20
Indonesia	Repo Rate	3.50%	1.5%	2.0%	Cut	Feb-21
China	Loan Prime Rate	3.85%	1.1%	2.8%	Cut	Apr-20
India	Repo Rate	4.00%	6.3%	-2.3%	Cut	May-20
Mexico	Overnight Rate	4.25%	5.9%	-1.6%	Hike	Jun-21
Brazil	Target Rate	5.25%	8.4%	-3.1%	Hike	Aug-21
Russia	Key Policy Rate	6.50%	6.5%	0.0%	Hike	Jul-21
Turkey	Repo Rate	19.00%	19.0%	0.1%	Hike	Mar-21

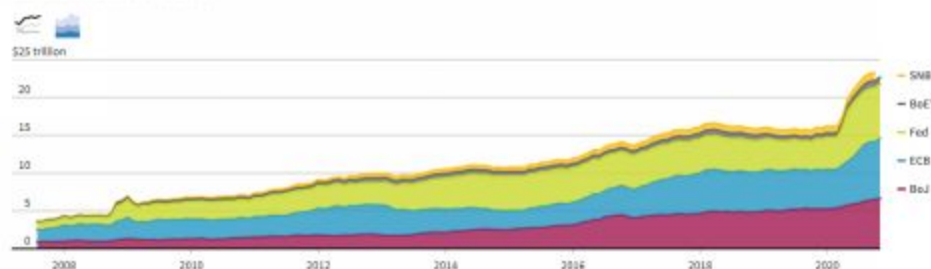
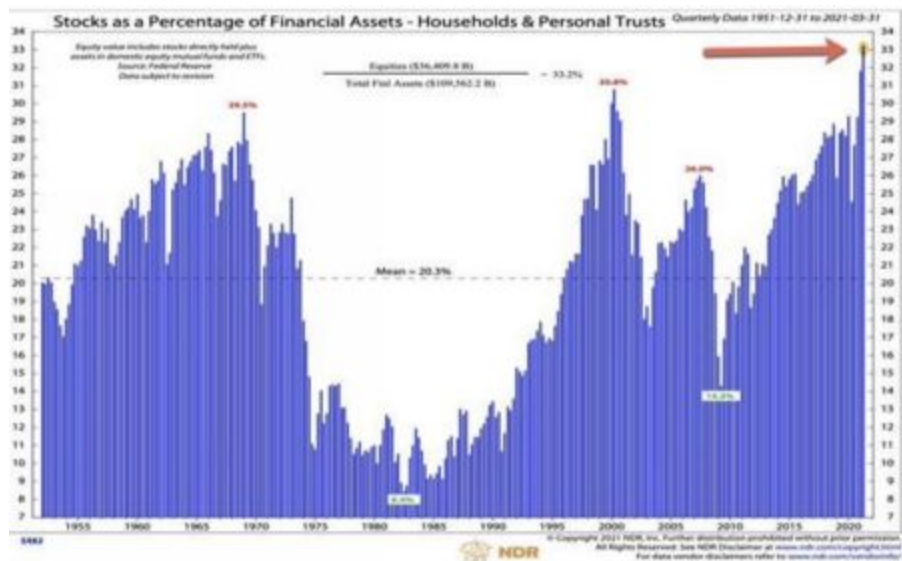
@CharlieBilello

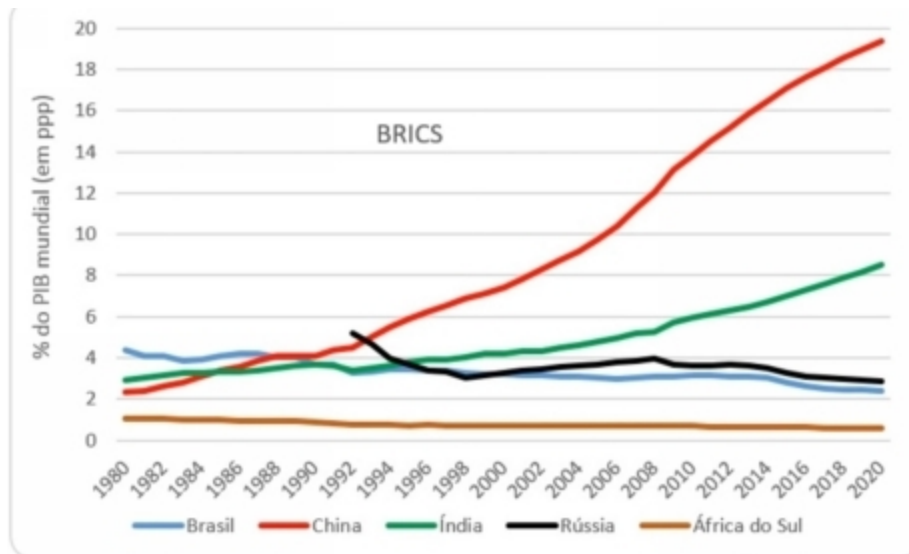
A história nos mostra que a corrupção dos sistemas monetários leva à decadência moral, colapso social e escravidão. A tentação de manipular dinheiro sempre se mostrou forte demais para a humanidade resistir.

@Breedlove22 *(Twitter)*

No mundo do dinheiro fiduciário, ter acesso às torneiras de dinheiro do banco central é mais importante do que atender clientes. As empresas que conseguem obter crédito com taxas de juros baixas terão uma vantagem persistente sobre os concorrentes que não conseguem. Os critérios para o sucesso no mercado tornam-se cada vez mais relacionados à capacidade de garantir financiamento a taxas de juros mais baixas do que à prestação de serviços à sociedade.

(O Padrão Bitcoin)

A expansão da estatização de ativos assusta[259]. Bancos centrais quintuplicaram ativos (estatização de mercados) em menos de 12 anos e hoje estatizaram mais de 50% do PIB dos seus respectivos países[260] (enriquecendo amigos do rei, multiplicando número de bilionários e explodindo desigualdade social):

Ações mais caras desde sempre

Metade do crescimento mundial entre 2008 e 2019 foi na China
Quase tudo devido a juro negativo e tolerância aos crimes da ditadura:

Fonte: Fundo Monetário Internacional (FMI) – visitado em 12/04/2016
(Nota: 2016 a 2020 = projeção) http://www.imf.org/external/datamapper/index.php

Ampliados diversas vezes os agregados monetários (quantidade de moeda) e os estoques de dívidas mundiais (públicas e privadas) e inflados os valores de ativos (imóveis, títulos e ações, por exemplo), dois cenários são resultantes: 1) a normalização dos juros acarretaria uma explosão no custo de endividamento dos Estados (já deficitários) e uma desvalorização brutal dos ativos (já que sua avaliação é, normalmente, feita por fluxo de caixa descontado por taxa de juro), resultando em colapso agudo das contas públicas e das moedas estatais; ou 2) a manutenção sistemática de juros negativos, com o empobrecimento também constante de quem investir no sistema sem ter acessos políticos para se beneficiar de captura administrativa, resultando no colapso crônico da poupança privada.

Conclui-se que o sistema financeiro convencional, *legacy*, tem seus dias contados até que ocorra uma correção que deve acabar ou tornar insignificantes a maioria das moedas, empresas e governos do presente – como asseveram Peter Schiff, Mike Maloney e Max Keiser ao afirmar que a próxima crise será maior que a de 2008, a de 1998 e até mesmo a de 1929.

Quem investiu na bolsa americana no topo de 1929 só se recuperou (ajustado pelo *CPI – consumer price index*) 52 anos depois[261]. Após 63 anos, quem investiu no topo ainda estava com ZERO GANHO e perda em

mais de 80% do tempo. Isso é a bolsa americana, onde há lei e governança para que mercados mobiliários sejam viáveis:

Em suma, é comprovada a perda das qualidades aristotélicas de dinheiro (capacidade de reserva de valor, fungibilidade, transportabilidade, divisibilidade e durabilidade) das moedas fiduciárias emitidas pelos governos, que só circulam devido ao curso forçado – ameaça violenta – até mesmo em decorrência de experimentos de demonetização e guerra ao dinheiro (proibições e restrições ao uso e posse de dinheiro em espécie, que abundam por todo o mundo).

É crescente o entendimento do "bug do ouro"[262], como detalhado por Micaroni, evidente nas diversas vezes em que o ouro privado foi expropriado, como já aconteceu até nos EUA e hoje ocorre na Índia e na Venezuela[263] – e nas restrições crescentes ao seu uso e transportabilidade.

3.1.1 Bitcoin, Ouro e Fiats no espaço tempo

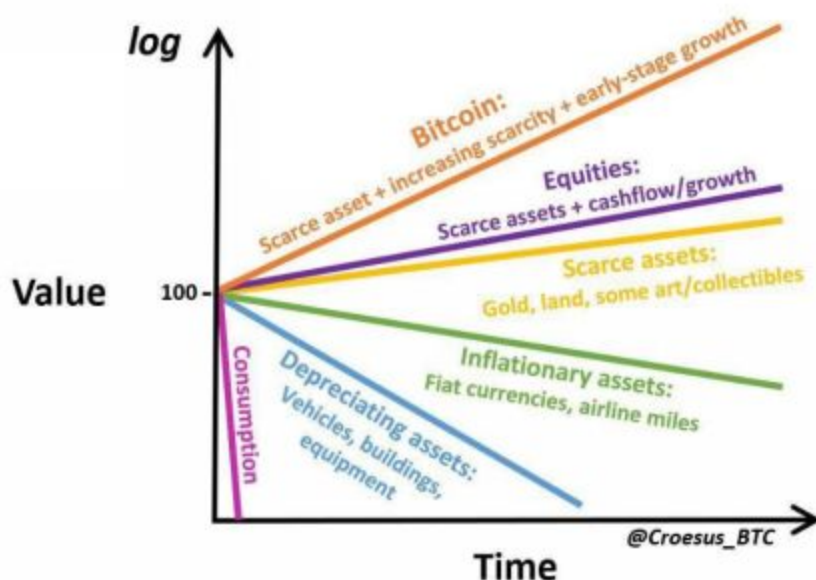
Os Bancos Centrais, quando imprimem mais *fiat*, diluem o valor de todos que possuem a moeda que eles emitem. Sua política econômica expansionista destrói riquezas acumuladas ao longo do tempo. Já na década de 1930, Henry Ford[264] afirmava que se a maioria das pessoas

entendessem como funciona o sistema monetário e bancário: “haveria uma revolução antes do próximo amanhecer”.

Optar pelo Bitcoin é sair do jogo fraudado no qual o honesto não tem como vencer — sem violência. É a alternativa crescente para armazenar, transportar e manter valor no espaço e tempo.

Ouro transporta valor bem no tempo, mas é péssimo no espaço, como ficou claro com quem guardou o metal em Cuba, Vietnã, Venezuela ou outro lugar tomado por ditadura comunista. *Fiats* transportam valor bem no espaço e são péssimas no tempo.

Bitcoin é bom em transportar na escala, no tempo e no espaço. A tendência é que seja, cada vez mais, eficiente em divisibilidade, transportabilidade e durabilidade: mais *halvings e* mais legitimação aumentam sua propriedade de reter valor no tempo (ou até ganhar). Mais soluções (2ª camada, *sidechains*, *offchain*, *etc..)* reduzem os custos de transação, ficando ainda mais transportável, divisível e fungível.

É urgente o amplo acesso a um dinheiro sólido em escala[265] (divisibilidade), espaço e tempo (*sound money)*. Mesmo os bancos já tomaram prejuízos bilionários com falsificação de ouro[266] demonstrando a complexidade para afirmar sua veracidade.

A solução de centralizar a sua custódia nas mãos de governos *(Gold Standard)* e terceiros de confiança foi tentada diversas vezes, mas sem sucesso. Todas as vezes as promessas de conversão, cedo ou tarde, foram desonradas[267].

O Bitcoin pode se provar como uma alternativa viável para o armazenamento de valor, melhorando as deficiências do ouro na propagação no espaço e no tempo. Imune à censura, pode ser enviado para qualquer pessoa no mundo a um custo relativamente baixo ou quase zero pela Internet.

Ouro e Bitcoin podem e devem coexistir. Mesmo que o ouro seja completamente desmonetizado, ele ainda terá valor como insumo industrial.

Alternativas ao ouro físico são *tokens* de *stable* ouro — como PAX Gold (*IOU* de ouro que pode ser enviada pela Internet); e, potencialmente,

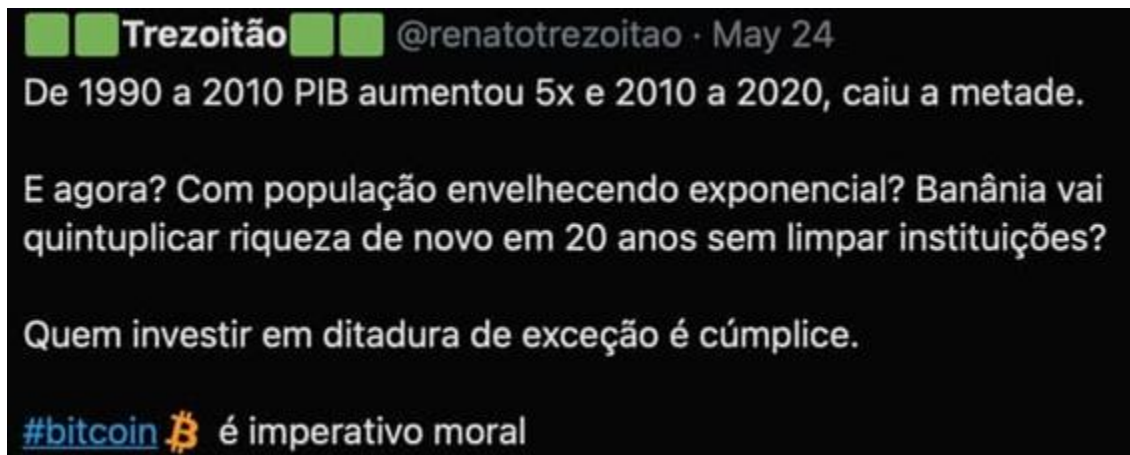
créditos de ouro gerados com colateral de bitcoin (como o *MAKERDAO* gera DAI, *stable* de dólar colateralizado em *crypto*).

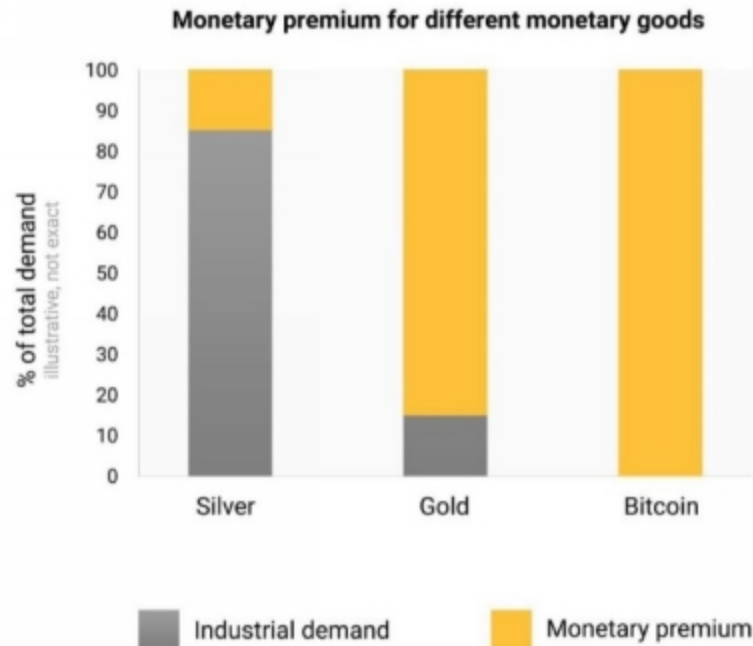
O bitcoin é o colateral supremo, simplesmente porque sua movimentação pode ser verificada publicamente e a sua posse comprovada com baixíssimo custo, por assinatura de chaves.

Se você pega um empréstimo colateralizado da Rispar[268] — ou com sua avó que depende da renda em real, pagando a ela 2 a 3x mais que o CDI (juro real negativo, coitada), quem pega os reais emprestados pode verificar onde os seus bitcoins estão depositados — até mesmo fazendo prova pública de infiel depósito ou estelionato se forem movidos de maneira diversa ao contratado.

Em decorrência disso, grande parte do ouro negociado no futuro, em vez de “ouro de papel” ou “ouro fisico" (com altíssimos riscos de transação, em transporte, certificação e inadimplência) tende a ser “ouro sintético”, colateralizado em bitcoin, aumentando ainda mais a demanda por BTC.

A rede *blockchain* do Bitcoin é um sistema de comunicação a prova de censura que possibilita diversas aplicações. Contratos e fatos podem ser registrados na blockchain[269]. A rede, portanto, transporta informações no espaço e tempo de forma segura — e não apenas ativos.

Em poucos anos a riqueza das famílias será mais determinada pelo ano em que começou a acumular BTC do que por sua profissão ou riqueza em outros séculos. Esse será o *RESET* para zerar riquezas obtidas de maneira ilegítima — exatamente devido à tendência sistemática de as elites morais e intelectuais aderirem ao padrão Bitcoin primeiro. Um filtro moral para quem for manter riqueza. Bitcoin é um imperativo moral e pragmático: investir no *legacy* (perda fixa e perda variável) é suicídio financeiro e moral, além de financiamento de crime.

3.1.1.1 Ouro ou Bitcoin? Ou ouro e bitcoin?

O ouro foi a reserva suprema de valor, histórica e global, com um valor total de mercado (*market cap*) de cerca de US$ 12 trilhões[270]. O emprego como reserva multiplica o valor de mercado do ouro muito além do valor derivado da sua utilidade industrial. O metal foi um ativo culturalmente importante por milhares de anos, devido às suas propriedades superiores de dinheiro sobre os demais metais e meios circulantes.

No entanto, o ouro tem algumas desvantagens importantes, nas quais se incluem:

a) **É difícil de transportar e caro armazenar**; exemplo disso é o deságio mais de 50% no preço na Venezuela e em lugares com controles draconianos[271]; e

b) **É difícil verificar qualidade e veracidade**[272], como resultado, grande parte do ouro do mundo é mantida em repositórios centralizados que seguem diretrizes rígidas[273] – e a maior parte do ouro vendido não tem liquidação física, não servindo de *hedge* nas situações de colapso societal. Um dos problemas do padrão-ouro (*gold standard*) é a impossibilidade de verificar os saldos e a conversibilidade dos depósitos. Essa deficiência é mitigada no Bitcoin, já que os saldos são públicos. Em um depósito consignado de bitcoin, é pública a prova de se os saldos foram ou não movidos e, assim, se estão ou não sob o controle do detentor de certo endereço.

c) **Ouro não é facilmente divisível**. A maior parte do ouro é entesourado na forma de barras, moedas ou joias, o que dificulta a transferência de quantidades exatas. Um grama de ouro, em maio de 2020, custava mais de R$ 300,00. Mesmo nas épocas em que o

ouro era moeda corrente, raras eram as pessoas que teriam a capacidade de fracionar, medir e guardar 30 reais em ouro, daí um dos motivos da monetização da prata e dos trocos de cobre.

O Bitcoin foi criado para emular e melhorar as propriedades que fazem do ouro reserva de valor, como descrito na narrativa de Ouro 2.0, também resolvendo alguns dos inconvenientes do ouro:

a) **Bitcoins são muito fáceis de transportar e armazenar:** Já houve transações nas quais foram transmitidas dezenas de milhares em bitcoins (avaliados em mais de um bilhão de dólares) ao custo de alguns dólares. Esse custo da transação (*fee*) é voluntário, quanto maior o valor pago, maior a chance de a transação ser processada rapidamente, quem tem pressa paga mais, quem não tem paga menos, e, em ambientes *off-chain* e de segunda camada, paga nada ou quase nada por transações imediatas, mas sem os registros públicos perpétuos e o mesmo nível de segurança. Várias corretoras, inclusive brasileiras, permitem trocas de saldos de bitcoin gratuitamente entre a *Lightning Network* e a *main-net*. Armazenar bitcoins é praticamente gratuito, se o titular memorizar as palavras geradoras (*seed phrase*) criadas *off-line* com senha criptografada (*brain wallet* ou *paper wallet* criptografada), então não há como roubar ou *hackear* os bitcoins sem o fornecimento da senha. O custo de usar *softwares* abertos e gratuitos não pode ser comparado com dispendiosos sistemas de cofres e monitoramento. Há dezenas de *wallets* (carteiras) gratuitas para *desktop* ou *smartphone* que acessam rapidamente os saldos quando importadas as palavras geradoras (*seeds*) ou chaves privadas. Por isso, em lugares como a Venezuela[274] , há deságio de ouro e ágio de bitcoin.

b) **Bitcoins são facilmente verificáveis:** Informações sobre cada bitcoin e saldos de cada endereço podem ser vistas na *blockchain* pública do Bitcoin, visível por qualquer pessoa conectada à rede. Os proprietários de bitcoins podem facilmente provar que os controlam (registro de propriedade), inclusive sem movimentar saldos e sem custo, através de assinatura de mensagens com a

chave privada (feita de maneira prática e segura por meio de *hardware wallets* ou gratuita e menos segura por programas gratuitos).

c) **Bitcoin é facilmente divisível**: A menor unidade de um bitcoin – batizada de *satoshi* pela comunidade – é cem milionésimos de um único bitcoin (0,00000001 BTC), portanto é divisível *on-chain* até a oitava casa decimal e é ainda mais divisível *off-chain*, como saldos em corretoras – essas frações de *satoshis* podem ser transacionadas também em segunda camada, como na *Lightning Network*[275].

É crença dos autores que mercados de *tokens* de *stable* ouro (e demais índices e *commodities* significativos), integralmente colateralizados em bitcoin, serão ativos superiores a ouro físico no futuro, tendo mais liquidez, transportabilidade e utilidade para colateral em empréstimos e alavancagem – finalmente resolvendo os problemas do padrão-ouro.

Os *tokens* atualmente oferecidos de *stables* (dólar, ouro ou qualquer outro bem), se não forem integralmente colateralizados em cripto (como *DAI* do *maker DAO*), apresentarão riscos de custódia compostos (do emissor, da *blockchain* em que estão registrados e de onde estiverem depositados) e estímulos ao oportunismo os inviabilizarão no longo prazo.

Classificação das principais características dos ativos: Bitcoin, Ouro e Moeda fiduciária[276]:

	Bitcoin	Gold	Fiat
Durable	B	A+	C
Portable	A+	D	B
Fungible	B	A	B
Verifiable	A+	B	B
Divisible	A+	C	B
Scarce	A+	A	F
Established History	D	A+	C
Censorship Resistant	A	C	D

O Bitcoin é um candidato emergente a ouro digital. Levará tempo e um histórico de desempenho em vários ciclos de mercado para que o Bitcoin seja amplamente considerado como uma reserva de ativos de valor equivalente ao ouro físico.

Como é natural na evolução de ativos monetários em suas funções (meio de troca, reserva de valor, unidade de conta...), as narrativas sobre o bitcoin têm evoluído: na primeira, o sistema era visto como meio de pagamentos barato e rápido, para substituir as moedas fiduciárias.

Na segunda Era, com aumento das *fees* e da cotação, a narrativa dominante passou a ser a de moeda para usos mais nobres, como remessas imunes a controles de capitais ou pagamentos com certo nível de privacidade (para mercados como *silk road*).

No terceiro ciclo, dominava a narrativa de ouro digital, com as identificações de padrões de valorização exponencial (como o *bitcoin rainbow chart* e o *S2F*[277]).

Na quarta Era, o bitcoin é considerado como ativo financeiro essencial para diversificação e aumento de potência de carteiras, dados seus índices de risco/retorno[278] e correlações; assim como, com a legitimação do BTC (demonstrada pelo desenvolvimento de mercados futuros, participação institucional e regulação crescente).

Diversos bilionários (como Peter Thiel, Jack Dorsey, Chamath Palihapitiya, Tim Draper, Mike Novogratz, Michael Saylor e outros) e personagens respeitados em mercados convencionais (como Ray Dalio[279] e Paul Tudor Jones[280]) recomendaram e admitiram ter adquirido bitcoins como meio de elevar rentabilidade por diversificação.

TEXAN HODL @TexanHodl · 4h

Ray Dalio 1 month ago: The US Government will ban bitcoin.

Ray Dalio today: I'd rather own bitcoin than a bond.

The tides are turning 👀

4. (How, How Much?) Como e quanto?

O Bitcoin resolveu de forma não violenta o consenso do “Problema dos Generais Bizantinos”[281], conhecido como “Falha Bizantina”[282], na área da computação, por meio da mineração por prova de trabalho (*Proof of Work - PoW)*[283].

O sistema resolve a questão de qual bloco reconhecer se dois mineradores emitirem simultaneamente informações diferentes, reconhecendo como válida a cadeia que apresentar maior prova de trabalho. É isso que o consenso de Nakamoto utiliza para resolver o problema dos gastos duplos: maior prova de trabalho. Por isso, quanto maior *hashrate*, mais caro é um ataque viável à rede, em termos de energia elétrica a ser empenhada executá-lo.

A partir de 2020, o bitcoin se tornou a forma de dinheiro mais escassa já inventada, momento em que sua inflação passou a ser menor que a do ouro (percentualmente, os novos bitcoins adicionados ao estoque já existente representam menos do que o novo ouro minerado em relação a todo o ouro que existe). Sua valorização contribui ainda mais para tornar a sua rede mais segura e imune a ataques.

Mais indicações do porquê o Bitcoin manter uma dominância altíssima dentre as criptos são: maiores Efeito Lindy[284] e Efeito Rede[285]; maior respeito à Lei de Gall[286] (mantendo complexidades e vulnerabilidades consequentes fora da camada base); e, por que, nas análises fundamentalistas de cripto, o *hashrate* é usualmente indicado como elemento inicial. O bloco com menor prova de trabalho e as transações nele contidas serão posteriormente reprocessados (se já não estiverem na *blockchain*).

O Bitcoin, como rede descentralizada, remunera os mineradores (com os valores das *fees* e dos novos bitcoins) pela capacidade computacional despendida (medida pela prova de trabalho).

Ele funciona com geração de estímulos de mercado que regulam a atuação dos mineradores (investindo mais ou menos em energia elétrica e equipamentos a depender dos seus custos de operação e da cotação do bitcoin, gerando um mercado mundial de energia elétrica, mesmo que produzida longe dos polos de consumo tradicionais); e dos usuários (investindo mais ou menos em *fees* e buscando mais ou menos soluções

alternativas de pagamentos, como a *Lightning Network*, *Liquid* e transações *off-chain*).

4.1 Bitcoin e o gasto de energia

Há amplas alegações[287] de que a mineração por *PoW (proof of work)* é um desperdício e prejudicial ao meio ambiente. Essa argumentação é puramente mentirosa[288]. A maior parte da energia utilizada na mineração é renovável e limpa (em muitos casos é energia ociosa, que seria desperdiçada), subsidiando a produção e distribuição de mais energia, com economias de escala e escopo.

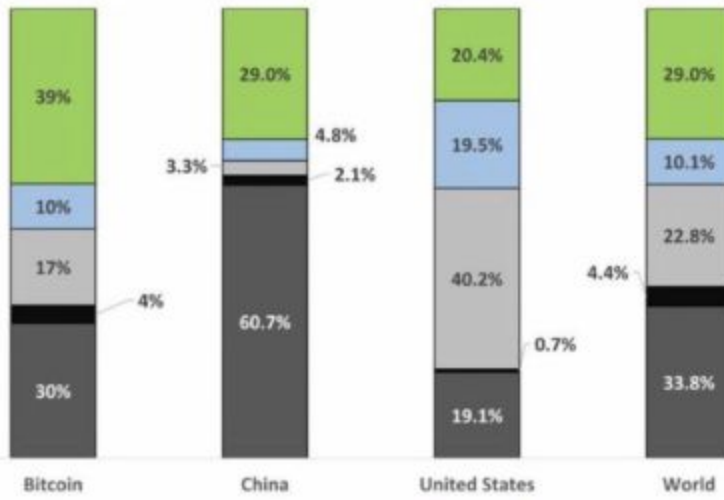
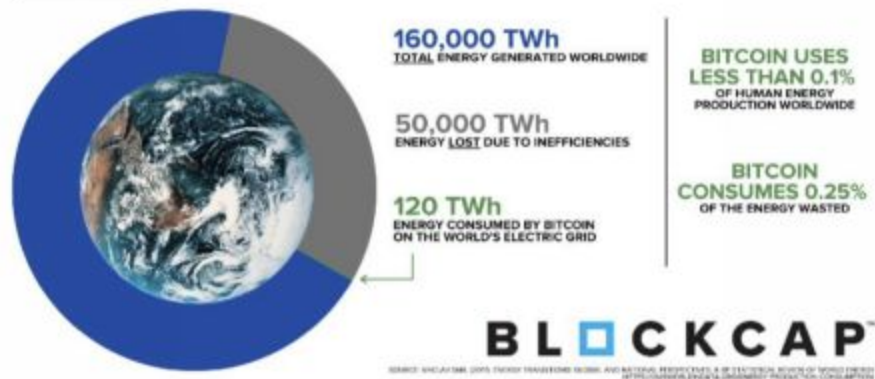
Mineração garante valor piso de energia, viabilizando projetos (inclusíve os de energia renovável) uma vez que estabiliza demandas intermitentes e reduz risco de não haver demanda local suficiente – além de previnir custos (institucionais, energéticos e ambientais) da mineração de ouro, da impressão de notas e manutenção de instituições bancárias.

Mesmo que essas refutações não fossem verdade, quem define o melhor uso de qualquer bem é seu dono. Se há pessoas dispostas a empregar seus recursos em bitcoins[289] e há pessoas dispostas a empregar seus recursos em máquinas e instalações para minerar bitcoins, está provado que o sistema é otimizado pelos mecanismos de mercado.

De fato, o Bitcoin hoje já consome mais energia[290] que países com milhões de habitantes, só que a questão ambiental deve ser considerada em termos de custos de oportunidade: qual o custo ambiental da produção do ouro (majoritariamente usado para reserva de valor), além do custo energético com a destruição do solo e contaminação química de cursos d'água? Para onde iria a energia ociosa? O custo mundial da energia cairia ou subiria se não houvesse o mercado de mineração de bitcoin garantindo um nível mínimo de remuneração pela energia, sem demandar qualquer infraestrutura de transmissão até centros urbanos ou industriais?

Carros consomem mais energia que carroças – que consomem mais que caminhar. Computadores consomem mais energia que máquinas de escrever – que consomem mais que caligrafia à mão. A evolução tecnológica normal é de mais consumo de energia em soluções superiores. Quem for realmente sincero em sua intenção de reduzir consumo de energia deve parar de usar computadores, máquinas de lavar, geladeiras e utensílios domésticos elétricos em sua casa, para começar.

Segundo diversas fontes[291] o Bitcoin é a indústria mais limpa do planeta e consome menos de 0,25% da energia ociosa (desperdiçada):

Electricity Mix (2020) - Bitcoin vs. China vs. USA vs. The World
39%
10%
17%
4%
30%
29.0%
4.8%
3.3%
2.1%
60.7%
20.4%
19.5%
40.2%
0.7%
19.1%
29.0%
10.1%
22.8%
4.4%
33.8%
Bitcoin
China
United States
World
Sources:
CBECI.org
ourworldindata.org/electricity-mix
Coal
Oil
Gas
Nuclear
Renewables (Incl. Hydro)
Hass McCook, May 2021, @FriarHass

Estimativas[292] indicam que as transações na *Lightning Network* são 3,7 milhões de vezes mais eficientes (em consumo de energia) que uma transação usando cartão de crédito. A economia *onchain* medida em W/GH (*Watts por Gigahash*) aumenta sistematicamente:

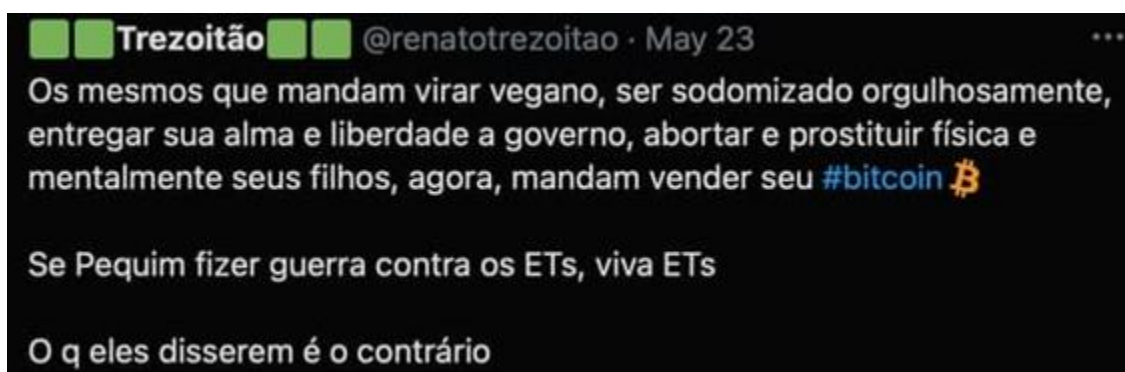
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Hash Rate (Gh/s)	0.003	0.575	0.550	0.650	63	878	4,255	9,750	11,500	22,550
Watts	55	241	271	250	445	509	1,145	1,200	1,450	1,786
Price (Release)	104	540	369	550	1,299	460	1,553	1,494	1,100	1,709
Efficiency (Gh/W)	**0.00005**	**0.002**	**0.002**	**0.003**	**0.16**	**1.7**	**3.7**	**7.9**	**7.9**	**12.4**
y/y		*4749%*	*-14%*	*27%*	*6190%*	*923%*	*121%*	*112%*	*1%*	*56%*
Hash Rate Cost ($/Gh)	**$39,808**	**$938**	**$671**	**$846**	**$21**	**$0.5**	**$0.4**	**$0.2**	**$0.1**	**$0.1**
y/y		*-98%*	*-28%*	*26%*	*-98%*	*-97%*	*-30%*	*-58%*	*-38%*	*-21%*

A classificação *ESG*[293]*(Environmental, Social and Governance)* é amplamente considerada forma de subversão[294] e sabotagem das economias do ocidente, vez que empobrece famílias e países.

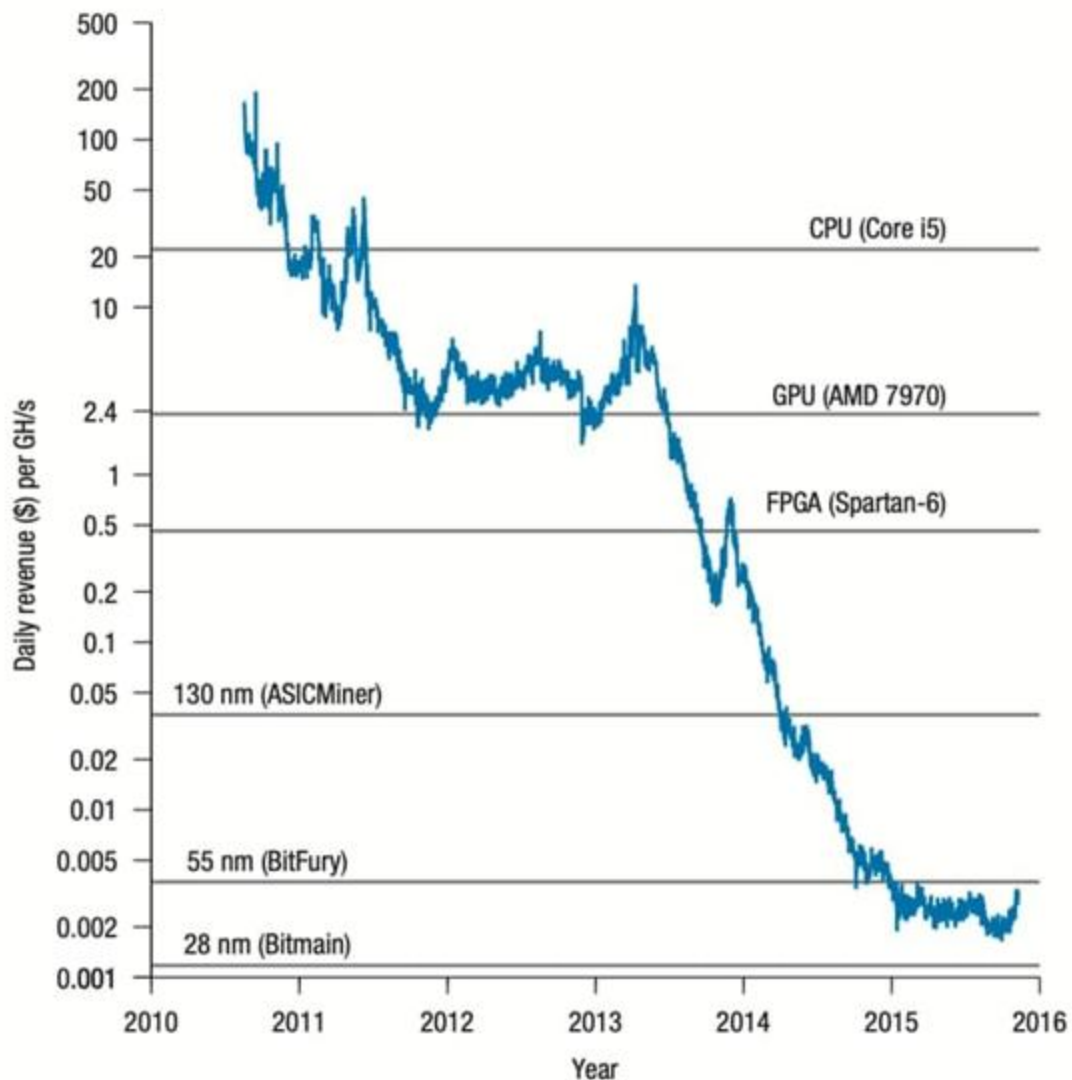
Com base nos dados sobre a mineração do Bitcoin, pode-se concluir que não há outra alternativa: a) mais benéfica ao meio ambiente (viabilizando economia de escala a projetos de produção de energia, ao resolver problema da energia ociosa e reduzindo uso de alternativas mais poluentes); c) mais benéfica à sociedade, porque resolve conflitos sem violência e gera riqueza e com a restauração de direitos individuais de livre expressão, de transação,

de propriedade e de acesso a dinheiro forte; e d) com governança superior (consenso não violento, com incentivos à cooperação).

Assim, qualquer alegação em contrário é um ataque de contrainteligência, com intuito de subverter sociedades, corporações, famílias e indivíduos – usando propaganda para fazê-los renunciar a tecnologia que os faria mais ricos e livres.

Exemplos de atos de guerra baseados em infiltração, subversão e contrainteligência – convencendo pessoas e instituições a ter comportamentos contrários aos seus próprios interesses e intenções são: o *financial welfare* da China[295] e "Coreia da Morte[296] contra os Estados Unidos — atraindo empresas com a promessa de acesso ao seus mercados gigantescos e baixo custos de operação a fabricar seus seus bens lá (para receber roubo massivo de propriedade industrial, expropriações e chantagens), o uso da Peste de Wuhan como arma biológica e de engenharia social[297]; ou mesmo financiamento público a militância anti patriótica racialista (como o projeto 1619 e o BLM) ou ao marxismo cultural dominante na academia ocidental[298].

Não faz diferença se a COVID foi fabricada e espalhada dolosamente, vazada culposamente ou foi criada e dispersada legalmente: se a ditadura comunista escondeu ilegalmente sua existência[299] (prendendo e torturando médicos que diziam a verdade, como Li Wenliang) e mentiu afirmando que se tratava de zoonose não transmissível entre humanos, inclusive usando OMS[300] aparelhada de militantes comunistas corruptos para confirmar narrativa, cada centavo gasto ou destruído com a fraudemia é responsabilidade dessa ditadura criminosa.

Outros exemplos atuais de ataques de engenharia social para convencer governos e populações a renunciarem a liberdade e riqueza são: a) *lobby* para países renunciarem a energia atômica; b) militância contra o consumo e produção de carne e proteína animal[301] (apenas veja o físico de Bill Gates[302]: com suas mamas, culotes e pança para concluir se ele pode te dar recomendações de saúde e alimentação); c) obrigatoriedade de focinheiras[303] de pano insalubres que aumentam transmissão de doenças por fômites; e, d) políticas de confinamento de saudáveis inocentes (*lockdown*) denunciada[304] por milhares de cientistas como totalmente prejudicial e sem qualquer evidência científica, empírica ou lógica, que a fundamente (além da intenção política de aumentar poderes e rendas dos donos do governo).

Retomando a questão da mineração, a evolução da eficiência dos *hardwares* que usam chips *ASIC (Application-Specific Integrated Circuit)* adaptados para minerar Bitcoin, com base em um algoritmo de *hash* específico, está diminuindo (assim como na indústria de *hardware* em geral, a Lei de Moore não é mais constante). À medida que a vantagem competitiva de estar no estado da arte diminui, podemos esperar um aumento na concorrência dos fabricantes, à medida que as margens diminuem, como podemos ver na imagem[305]:

Quando a energia usada para *PoW* * irá * parar de crescer? Precisamente quando produtores de energia suficientes começarem a fazer *PoW* diretamente, o retorno marginal da queima de kWh de energia através de *PoW* = o retorno marginal da venda desses kWh à rede – quando o “prêmio” no *PoW* é

> reduzido a zero. Eu chamo esse equilíbrio de "ponto de Nakamoto". Suspeito que o *PoW* usará entre 1 e 10% da energia do mundo quando esse equilíbrio for alcançado.
>
> Dhruv Bansal[306]

> Alguns reclamam que a mineração de Bitcoin não realiza "nada de útil", como encontrar números primos. Embora a introdução de uma recompensa secundária por fazer o trabalho possa parecer uma ideia virtuosa, na verdade, introduz um risco de segurança. Dividir a recompensa pode levar a uma situação em que "vale mais a pena fazer a função secundária do que fazer a função primária". Mesmo se a função secundária fosse inócua (um aquecedor), em vez de US $ 100 por x *hashes*, nós passaríamos para US $ 100 + US $ 5 de calor por x *hashes*. O "Aquecedor de Mineração" é apenas mais um aumento na eficiência do hardware, resultando em uma maior dificuldade e um aumento em (energia utilizada / bloco). Felizmente, o Bitcoin nunca terá esse problema, pois sua segurança é garantida pela pureza de seu algoritmo de prova de trabalho.
>
> Noah Ruderman

4.1.1 Bitcoin, otimização de energia e desinformação

Além de Elon Musk, outros magnatas do setor de energia estão investindo e estudando o potencial do Bitcoin, como alternativa de reserva de valor e meio de demanda constante, garantindo valor “piso" da energia gerada, mesmo a ociosa, que seria perdida de outra maneira.

Exemplos são Carl Icahn e Røkke, CEO da *Aker*[307]. A *Aker* criou uma subsidiária, *Seetee*, dedicada ao investimento em Bitcoin e projetos relacionados ao ecossistema. A nova unidade promete uma estratégia tripla: investir em bitcoin como seu ativo de tesouraria, investir em projetos e empresas cripto e implementar operações para a mineração de bitcoin.

Em carta[308] aberta aos *stakeholders* da *Seetee*, Røkke comenta como o bitcoin pode ser a forma de "bateria" definitiva para viabilizar energias alternativas intermitentes (como solar e eólica). Quando os componentes do

hardware de mineração virarem *commodity*, qualquer energia ociosa, em qualquer lugar do mundo, poderá ser convertida em bitcoin.

Nessa carta, o presidente da Aker fez afirmações interessantes:

> A criação da *Seetee* é resultado de uma discussão longa e fundamental sobre valor e acredito que o Bitcoin é superior ao dinheiro físico e ainda melhor do que o ouro. […] Estamos acostumados a achar que o dinheiro físico é livre de riscos. Mas não é. É explicitamente taxado pela inflação com uma pequena taxa a cada ano. […] O bitcoin é como o ouro, mas bem melhor. […] As pessoas que mais sabem sobre Bitcoin acreditam que seu sucesso futuro seja quase inevitável, enquanto o outro lado acha que seu fracasso é quase certo. A situação atual não é possível. [livre tradução]

Um *whitepaper*[309] lançado pela *Square* (empresa de pagamentos de Jack Dorsey) com a participação da *Ark Invest*, intitulado "Bitcoin é a chave para um futuro de energia limpa e abundante", propõem que o Bitcoin é o caminho para um futuro sustentável. O *paper* foi lançado como parte da *Bitcoin Clean Energy Initiative*[310].

Há também estudos interessantes sobre consumo de energia do Bitcoin, feito por empresas importantes do setor como a *Coinshares*[311] e *Galaxy Digital*[312].

Como resta evidente, o Bitcoin funciona majoritariamente com energia ociosa e pode até ser considerado uma "bateria global". Mesmo quando não é utilizada energia energia ociosa, não há retirada de energia usada em qualquer uso mais nobre, considerando que as margens de mineração são baixíssimas.

A mineração de Bitcoin aproveita energia desperdiçada, mitiga a destruição de capital e fornece um mecanismo para comercializar energia limpa e renovável onde quer que a encontremos. Com a tecnologia atual, as energias renováveis não podem substituir os combustíveis fósseis (hidrocarbonetos) por completo sem impactar brutalmente no padrão de vida da humanidade – como ficou evidente na crise energética do Texas em 2021[313].

Painéis solares, pás (ou hélices) de usinas eólicas e baterias também apresentam impactos ambientais brutais[314], usualmente ignorados no debate público – devido aos custos de sua fabricação e de descarte.

A febre dos carros elétricos – sejam alimentados por baterias ou por células de hidrogênio – também é uma distorção resultante dos juros negativos e de captura administrativa, corrompendo políticas públicas. Esses veículos nunca foram viáveis sem quantidades brutais de subsídios – e talvez não sejam em décadas.

Defender um sistema baseado puramente em energias renováveis[315] significa defender energia mais cara e menos oferta de energia, tornando a sociedade mais dependente e pobre. Em regra, uma rede totalmente dependente de energias renováveis coloca a sociedade à mercê do clima favorável ou de importação de energia – como ficou claro na Alemanha, com energia caríssima e prostrada em submissão aos vizinhos, dos quais depende de importação[316].

O Bitcoin contribui para que novos projetos sejam desenvolvidos e viabilizados garantindo demanda fixa com preço mínimo. Toda infraestrutura de mineração de bitcoin também pode se beneficiar da energia nuclear, tida também como não poluente[317] em que os rejeitos são, cada vez mais, recicláveis[318]. Até mesmo bilionários globalistas como Bill Gates, investem pesadamente em projetos de energia nuclear[319].

Existe ainda uma batalha árdua sobre o combate à desinformação sobre a mineração de bitcoin, por isso muitos na comunidade produzem diversos artigos, vídeos e livros para desmistificar a mentira de que "o bitcoin é deletério para o meio ambiente”.

Outro movimento de desinformação é o *"The Great Reset"*[320] promovido por organizações globalistas[321] com o objetivo declarado de promover reengenharia social e econômica mundiais. Segundo eles, a “única saída" para crise do Covid-19 (“pandemia”) é um “mundo melhor” no “novo normal”, como a redefinição do contrato social (o Estado interferindo ainda mais na vida das pessoas, ou seja, socialismo implementado por meio de mais controle) e a agenda ESG *(Environmental, social and corporate governance*)[322] juntamente com a agenda ambientalista alarmista (como a descarbonização).

Um dos objetivos do "Grande *Reset"*[323]: "Você não terá nada e será feliz.”. Se discordar e quiser ter patrimônio, liberdade e honra, basta desinvestir do *legacy* e comprar bitcoin.

Bilionários (cantillonarios), celebridades (progressistas) e as elites[324] mundiais não querem que você possua nada e afirmam que você será feliz. Benjamin Franklin já dizia que: "Aqueles que abrem mão da liberdade essencial por um pouco de segurança temporária não merecem nem liberdade nem segurança."

4.2 Mineração, endereços e ajustes

O mecanismo de ajuste de dificuldade (entre *hashpower* e tempo médio de criação de blocos) da rede Bitcoin fornece correção necessária para os mineradores a cada 2016 blocos.

Se o *hashpower* (poder computacional) subir de maneira significativa até o ajuste, os blocos tenderão a ser produzidos em média mais rapidamente, aumentando a emissão diária de bitcoins – por isso, não há previsão exata dos futuros *halvenings* (porque dependem do número de blocos minerados e o tempo para que isso ocorra pode ser reduzido se houver aumentos repentinos de investimentos em mineração).

Os blocos são gerados a cada 10 minutos, em média. Tende a ser mais rápido quando o *hashrate* aumenta e, em sentido contrário, tende a demorar mais quando o *hashpower* total aportado na rede cai.

O ajuste de dificuldade é a tecnologia mais confiável que existe para produzir uma moeda forte e controlar a taxa de escassez. Sem esse mecanismo e com o poder de mineração aumentando exponencialmente, todos os bitcoins já teriam sido minerados.

Outro mito repetido por quem não compreende os mecanismos de ajuste entre mineração e preços de mercado é o “preço mínimo de mineração viável”, abaixo do qual haveria uma “espiral da morte”. Ora, se há mais empresas minerando, então os bitcoins emitidos vão ser divididos entre mais agentes.

Se a cotação do bitcoin cair brutalmente e metade dos mineradores deixarem de operar (devido a seu custo de operação ficar acima do valor dos bitcoins recebidos), as *fees* e os novos bitcoins (subsídio) serão divididos pela metade entre os mineradores que continuarem (aumentando sua remuneração até haver equilíbrio de mercado).

Então, se o bitcoin cair de 50 mil para mil dólares, a “morte” poderá acontecer para os mineradores com maiores custos de operação, mas, para os operadores de menor custo, a operação continuará viável, pois receberão mais bitcoins com menor valor unitário. O sistema se autorregula até o

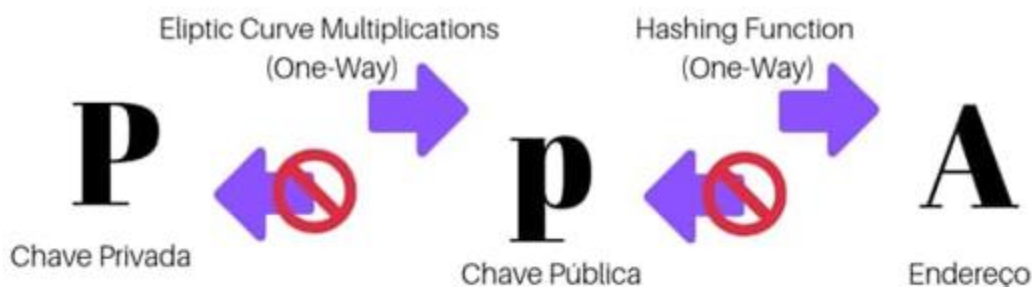
equilíbrio, a mineração continua sendo viável em algum nível com qualquer preço atual ou futuro positivo de bitcoin.

Se for considerado o fato de que agentes mineram para adquirir fluxo de caixa em bitcoin sem considerar custo de operação imediato – por exemplo, por *hobby* ou por já ter vendido os bitcoins em mercado futuro ou feito *hedge* com opções –, então, não existiria "preço mínimo de mineração", pois esses mineradores continuariam a operar independentemente da cotação corrente.

O Bitcoin permite a criação de chaves (públicas e privadas) e endereços *off-line* (sem acesso à Internet). Os endereços[325] são sequências alfanuméricas derivadas de chaves públicas para o recebimento de bitcoins.

Para movimentar os saldos ou comprovar sua propriedade com assinatura de mensagens, é necessário acessar as suas chaves privadas.

Os endereços são equivalentes às contas bancárias e as chaves privadas equivalentes às senhas para sacar ou transferir seus saldos.

Uma analogia didática ao funcionamento é o *e-mail*: quem souber seu endereço de *e-mail* pode enviar mensagens para esse endereço; e quem tiver a senha (chave privada) desse *e-mail* pode mandar mensagens a partir dele. A particularidade é que *e-mails* não podem ser criados *off-line*, como endereços de bitcoin[326]:

O bitcoin é divisível por possuir seu próprio sistema de unidade de medida, dotado de até oito casas decimais, a última delas sendo nomeada

satoshi (centésimo milionésimo de bitcoin). Considerando uma cotação de 100.000 USD por bitcoin, um *satoshi* valeria 0,001 dólar, extremamente divisível.

Créditos de bitcoin, negociados em segunda camada ou *off-chain*, como na *Ligthning Network*, *t*ambém permitem transações de frações de *satoshis*, sendo ainda mais divisíveis nesses ambientes.

Há diversas propostas para aumento das casas decimais no futuro, quando o bitcoin valer milhões ou bilhões de dólares, demandando apenas alteração no protocolo através de *soft fork* ou *hard fork* a depender das questões técnicas, isso é proposto através de um BIP *(Bitcoin Improvement Proposal)* *[327]*.

As moedas tradicionais (dólar, real ou euro) costumam ser divididas apenas até sua centésima parte, o chamado centavo ou cêntimo. No caso do real, 1 centavo = R$ 0,01. Cada bitcoin tem apenas existência digital na rede de computadores que constitui o sistema Bitcoin, muitas das vezes representado por unidades como 1 mBTC, 1 *satoshi* ou 1 µBTC; mas a unidade que possui mais uso no sistema é o *satoshi*, homenagem a Satoshi Nakamoto, criador do sistema Bitcoin.

Na figura abaixo[328], apresentam-se as siglas, os nomes e unidades de medida do bitcoin:

1 Satoshi =	0.00000001 ฿	
10 Satoshi =	0.00000010 ฿	
100 Satoshi =	0.00000100 ฿	= 1 Bit / µBTC (you-bit)
1,000 Satoshi =	0.00001000 ฿	
10,000 Satoshi =	0.00010000 ฿	
100,000 Satoshi =	0.00100000 ฿	= 1 mBTC (em-bit)
1,000,000 Satoshi =	0.01000000 ฿	= 1 cBTC (bitcent)
10,000,000 Satoshi =	0.10000000 ฿	
100,000,000 Satoshi =	1.00000000 ฿	

O bitcoin é progressivamente (assintoticamente) mais escasso (emissão decrescente), pois sua política monetária é previsível, ao contrário do sistema monetário convencional, no qual os Bancos Centrais podem imprimir o quanto quiserem determinados por decisões políticas.

Nunca haverá mais de 21 milhões de bitcoins. Em abril de 2019, havia em circulação em torno de 18,3 milhões[329]. O último subsídio (novos

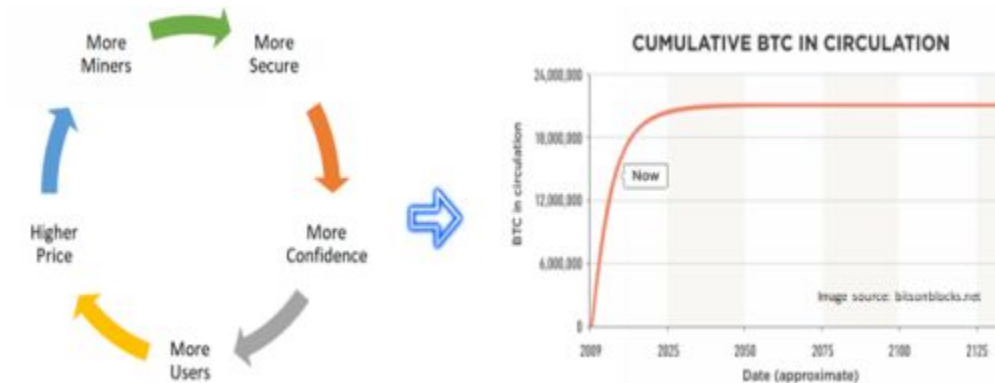
satoshis criados para remunerar mineradores) está previsto para ser minerado no ano de 2140 (quando se espera que o sistema continue funcionando apenas remunerado pelas *fees*, ou sejam introduzidas mais casas decimais para a emissão de subsídios). Sua emissão é controlada pelo algoritmo de código aberto desinflacionário que já existia desde sua proposta original.

Como Nick Szabo[330] denominou, um bem monetário deve ter “custo imprevisível”. Em outras palavras, o bem não deve ser abundante ou fácil de obter ou produzir em quantidade. A escassez é provavelmente o atributo mais importante de comparação entre reservas de valor (como no modelo do *S2FX – stock to flow cross-asset model*), pois, como demonstrado por *PlanB* (investidor institucional holandês), há correlação direta entre medidas de escassez (*S2F*) e *market cap total.*

Outro importante ensinamento do "mestre silencioso" Nick Szabo é que o segredo do sucesso do Bitcoin não está necessariamente relacionado a seu consumo prolífico de recursos ou à escalabilidade computacional, mas requer algo ainda mais valioso: a escalabilidade social *(social scalabity)* em seu *design*, através da segurança.

Escalabilidade social é a habilidade que uma instituição tem de alcançar um número maior de participantes em um esforço comum. Exemplos de instituições socialmente escaláveis (que reduzem custos de transação e conflitos entre usuários) são linguagem, lei e religião.

A figura abaixo[331] demonstra um modelo do círculo virtuoso mencionado em função de sua base monetária com inflação decrescente: o valor do Bitcoin seria atribuído a sua segurança (em vários níveis) derivada da sua descentralização e resistência à censura; que, por sua vez, reforçam a credibilidade da escassez, que é a base do armazenamento de propriedade de valor do bitcoin.

Descentralização e o cronograma de emissão

Por exemplo, deve ser muito difícil para qualquer participante ou intermediário criar dinheiro (para diluir a curva de oferta, levando a uma inflação indevida ou inesperada).

> Em resumo, todo o dinheiro que a humanidade já usou foi inseguro de uma maneira ou de outra. Essa insegurança se manifestou de várias maneiras, da falsificação ao roubo, mas a mais danosa dentre todas provavelmente foi a inflação.
>
> Nick Szabo

O bitcoin é, em diversos aspectos, o ativo mais transportável já criado e o primeiro dinheiro que pode ser transmitido por qualquer meio de comunicação. Para transacionar *onchain,* é necessária alguma conexão com a *internet*, mas transações *offchain* também são possíveis, por exemplo, com dispositivos como *Opendime*[332] da *Coinkite.*

Muitas vezes, ouro físico em território controlado por Estados falidos (como Coreia do Norte, Venezuela ou Cuba) não vale nem metade do que em mercados livres.

Onde há controle de capitais draconianos, não é viável sair legalmente com posse de ouro. A senha para acesso a seus bitcoins pode ser memorizada, enviada por carta, rádio, *e-mail* ou inserida em *hardwares* criptografados (ou até expressa em furos em um cartão como no caso da

Stackbit[333]). A única maneira de impedir o transporte de bitcoins é impedir toda a forma de comunicação.

O bitcoin é difícil de falsificar: por usar a rede *blockchain* para registro perpétuo de transações, o sistema se mostra inviável de ser adulterado permanentemente; até o momento o único problema[334] crítico que foi explorado ainda no início da rede (2010) foi o *bug*[335] que inflou[336] a oferta de bitcoins e que logo foi resolvido via *fork* juntamente com uma atualização de *patch* (correção de código)[337]; após terem resolvido toda a situação, os desenvolvedores entraram em contato com todos os mineradores da época e solicitaram que todos atualizassem as suas versões do *software* e retornassem as transações anômalas.

Maximalistas consideram *altcoins* como falsificações do bitcoin.

Não é possível criar um bitcoin falso sob quaisquer condições. O ataque conhecido como ataque de 51%[338], quando um atacante consegue obter mais de 51% do poder computacional da rede, só consegue desfazer transações, refazendo blocos já minerados.

Trata-se de ativo escasso que é armazenado em uma carteira digital, registrado na *blockchain* de forma publicamente auditável (análoga a um registro de propriedade), podendo ser acessado de qualquer lugar via uma conexão de Internet (ou *off-line* via novas tecnologias sendo aprimoradas, como a de acesso via satélite ou ondas de rádio).

Especialmente após os escândalos dos *Paradise Papers* e *Panama Papers*, das regulações como a *FATCA* e as padronizações de *compliance* como *KYC/AML* (*know your customer* e *anti-money laundering*), os paraísos fiscais e regulatórios para *offshores* se tornaram, mais e mais, inseguros e suspeitos: basta os dados vazarem ou a política oficial do país mudar que se pode perder tudo e todas as transações se tornarem públicas.

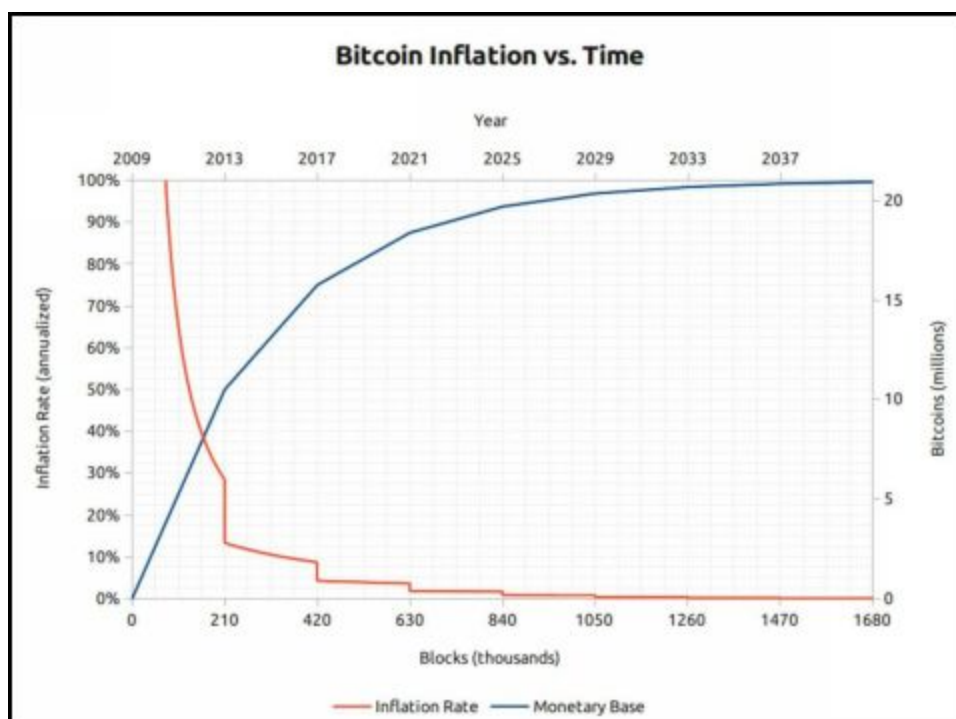
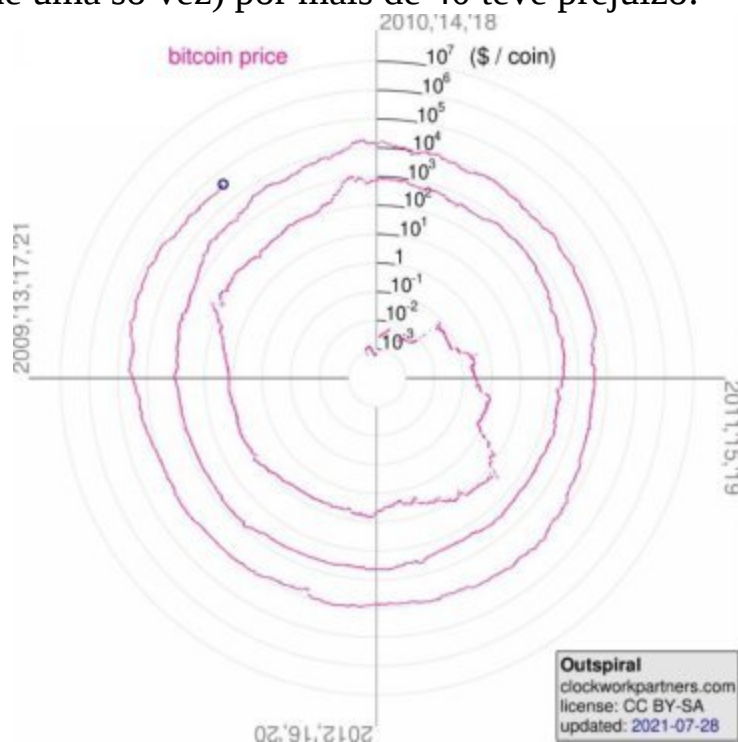
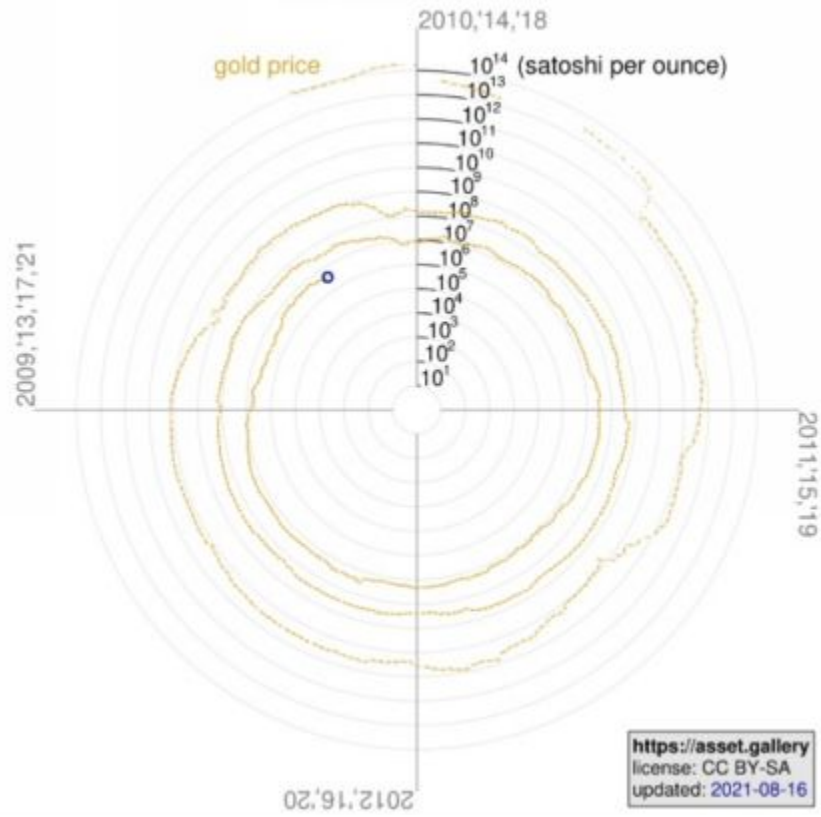
Saldos de criptomoedas podem ser memorizados, por exemplo, através das sementes (*seeds*) geradoras das chaves (12, 18 ou 24 palavras). Essas matrizes (ou as transações derivadas delas) podem ser enviadas por rádio, telefone, *e-mail* ou anotadas em qualquer pedaço de papel e que podem, por sua vez, ser criptografadas para que alguém que capture a mensagem não possa acessar o saldo. Por isso as *hardware wallets* mais seguras são *air gapped* (nunca acessam Internet e são fisicamente isolados). A transação pode ser feita com retirada com cartão de memória, como na *Coldcard* da *Coinkite* (ou pode ser feito até em *tablet* ou celular velho, baixando *wallet* q rode *offline*, como *Samourai*).

4.3. Halving do Bitcoin: política monetária

A política monetária do Bitcoin possui uma emissão desinflacionária predeterminada. Ou seja, a inflação é decrescente em ritmo logarítmico com emissão caindo à metade a cada 210.000 blocos ou 4 anos, aproximadamente, em um processo chamado *halving*[339]. Predeterminação de emissão e desinflação são os opostos das políticas monetárias da maioria dos governos.

Processo do Bitcoin *halving*, que irá torná-lo menos inflacionário até chegar próximo a sua oferta limite de 21 milhões (assintoticamente):

Evento	Data	Sequencial do bloco	Recompensa do bloco	Total de novos bitcoins entre os eventos
Lançamento do Bitcoin	3 de janeiro de 2009	0 (bloco Gênese)	50	10.500.000
Primeiro halving	28 de novembro de 2012	210.000	25	5.250.000
Segundo halving	9 de julho de 2016	420.000	12,5	2.625.000
Terceiro halving	11 de maio de 2020	630.000	6,25	1.312.500
Quarto halving	**Esperado para maio de 2024**	**840.000**	**3,125**	**656.250**
Quinto halving	Esperado para 2028	1.050.000	1,5625	328.125

A cada quatro anos, o número de bitcoins produzidos como subsídio aos mineradores é reduzido à metade. A emissão de novos bitcoins inteiros deve terminar, aproximadamente, em 2032, quando o subsídio será de 0,78125 BTC por bloco. Em 2140, aproximadamente, se não aumentarem as casas decimais, acabam os últimos *satoshis* de subsídio e o sistema terá que funcionar exclusivamente financiado por *fees*.

Os gráficos[340] seguintes de eixo radial e escala logarítmica plotam o preço do bitcoin dentro dos ciclos de 4 anos (cada ¼ de volta representa um ano) em US$ e ouro. O fato de a linha nunca ter cruzado demonstra que ninguém que tenha comprado e feito *hold* por 4 anos teve prejuízo nominal em *fiat*. Pelo contrário, em qualquer ponto analisado, o preço do BTC está a uma (10x) ou algumas (10^nx) ordens de grandeza maior do que no ciclo anterior. Se esse histórico for levado ao limite, ninguém que tenha feito *DCA* (compras parceladas recorrentes) por mais de 30 meses ou puro *lump sum* (compra de uma só vez) por mais de 40 teve prejuízo:

CAPÍTULO II: 10 OPERAÇÕES BÁSICAS - PRÓS, CONTRAS E CASOS

Existem basicamente três canais (*gateways*) para comprar bitcoin (análogas aquelas para comprar ouro): 1) Corretoras (*Exchanges* centralizadas e descentralizadas), 2) *OTC* (*over the counter*, mercado de balcão) e 3) *P2P (peer-to-peer* ou pessoa a pessoa, sem intermediários).

É possível adquirir bitcoins ou ouro por meio de aquisição original: mineração. Assim como, mendigando (*faucets*) ou sendo remunerado por algum serviço ou produto com esses ativos.

A melhor época para plantar uma árvore foi 20 anos atrás; o segundo melhor momento é agora. - Provérbio Zen

1) Mineração:

Consiste em ser remunerado por prover serviços de processamento de dados para *blockchain*. Forma de aquisição primária e original de cada bitcoin.

Hoje, essa atividade destina-se a grandes investidores, evitando a “maldição do vencedor”, dispostos a converter grandes fluxos de *fiat* (moeda fiduciária) em *bitcoin* sem pressa, comprando serviços de grandes empresas.

Operam onde há energia a baixos valores: ociosa, isenta ou furtada[341], criando um mercado mundial de "valor-piso" da energia, subsidiando investimentos em produção, mesmo longe de centros consumidores industriais ou urbanos.

No início, mineração doméstica era viável, mas logo passou a ser dominada por agentes munidos de estruturas industriais com *hardwares* especializados.

Além disso, em muitos casos, a mineração é executada pelos próprios produtores dos *hardwares*, ou agentes com ligações próximas a eles, pois receber um equipamento depois de meses de seu lançamento já pode inviabilizar o retorno do investimento.

Devido às margens dependentes da cotação, alguns equipamentos se tornam obsoletos em menos de 16 meses. É um negócio de alta complexidade, investimento intensivo, alta dependência de acesso privilegiado e margens comprimidas.

Como não fazer[342]: se não tem equipamento, energia elétrica e banda de Internet a preços competitivos, terá prejuízo. Mineração na nuvem nunca foi viável, e mineração doméstica, sem furtar energia e obter *hardware* a baixo custo, não é viável desde a segunda Era de subsídio de mineração. Muitas vezes, a mineração é pretexto para venda de "pacotes" de lucro garantido em esquemas Ponzi.

2) Acumulação (*hodling/hodl*) e análise fundamentalista:

"Holdar" consiste em adquirir bitcoins como reserva de valor, mantendo suas chaves em locais seguros (como *paper wallets* geradas *off-line*, de preferência criptografadas). *Hodlers[343]* (acumuladores) limitam seu uso a alternativas com vantagens financeiras significativas, como envios internacionais, elisão fiscal, doações e pagamentos a dissidentes[344] e aquisição de *gifts cards*, para substituição imediata.

Destina-se a investidores de qualquer porte que avaliem que os ganhos e os riscos nas demais atividades não compensam o seu custo de oportunidade.

Como não fazer: Adquirir bitcoins e deixá-los em posse de terceiros (saldos em empresas) representa alto risco não remunerado, evidente em dezenas de casos de perdas (*MtGox*, *Bitfinex*, *Atlas* e outros). Vendendo acima de 35 mil reais por mês por CPF em corretoras brasileiras, sai-se da faixa de isenção e deve-se pagar imposto de renda (IN 1.888/2019[345]).

Resultados: Existem estratégias particulares a cada perfil na constituição de uma carteira: a) em todos os prazos significativos, quem adotou prática de preço médio (*DCA - dollar cost averaging*)[346] multiplicou sua riqueza se continuou por mais de um ciclo (4 anos), ressalvando que nas calculadoras de DCA não consideram outros ganhos – nem com *lending*, nem *trade* nem mesmo *forks*; b) quem tem experiência em operações em outros mercados, tempo livre e baixa aversão a risco pode bater retornos do mero preço médio fazendo capitalização por aluguel ou *lending* – ou alavancando por colateralizado de *fiat* inferior; c) para quem tem controle emocional para comprar caindo e vender subindo (o que é muito mais difícil do que pode parecer), adotando análises fundamentalistas, gráficas ou de sentimento – como *mayer multiple*, *S2F/S2FX*, dados *onchain*[347] ou *google trends* indicando buscas por bitcoin — há estratégias ainda mais lucrativas que DCA (que já não é *hodl*).

Também há estratégias que apresentam ganhos em USD (e, consequentemente, em *stables*) e em bitcoin sobre o simples *holding*, embora haja também trabalho e riscos marginais envolvidos.

Outras formas de análise de fundamentos mais elaboradas sobre o Bitcoin são: a) número de artigos acadêmicos escritos sobre Bitcoin que podem quantificar a penetração nas universidades; b) número de projetos de código aberto que contêm a palavra "Bitcoin" em repositórios de código como o *GitHub,* uma medida muito valiosa, pois demonstra a capacidade de cérebros desenvolvendo novas ferramentas e projetos complementares em torno da rede; c) dados *on-chain*, a principal fonte de dados para analisar os fundamentos de base, como poder de *hash* empregado pelos mineradores que protegem a rede, número de transações, dentre outras informações que podem ser encontradas em sites como *blockstream.info, coinmetrics, glassnode e skew.*

Satoshi Nakamoto, o primeiro bilionário pseudoanônimo nunca pagou impostos sobre sua fortuna, não investiu mais que seu trabalho e computação domésticos e esperou o patrimônio adquirido ganhar valor com o tempo.

3) *Trade* com análise técnica (AT)

Consiste em comprar e vender bitcoin por *altcoins*, *stable coins* ou *fiat*, segundo indicações de análise técnica (padrões gráficos, indicadores e osciladores). Destina-se a investidores com formação e experiência em AT – ou dispostos a desenvolvê-las com estudo – e que queiram aumentar lucratividade dedicando seu tempo e arriscando seu patrimônio.

Como não fazer: seguir esquemas de *pump and dump* como canais do *Telegram*, investir em *altcoins* sem ler a documentação básica e acompanhar as fontes de notícias, ou concentrar parte substancial da carteira na mesma corretora. A maioria das *altcoins* tende a virar pó. A maioria das corretoras que existiram deram *exit scam* ou foram supostamente *hackeadas*, algumas mais de uma vez.

Como fazer: Estude AT e inicie com trocados. Abra contas em diversas corretoras para diversificação e mantenha registros de sua contabilidade para controle. Só avance em complexidade dos produtos – mercados futuros, operações alavancadas e derivativos – quando compreender completamente suas consequências.

Negociar com bitcoins é altamente indicado para quem já tem experiência negociando ações, *forex* ou títulos, pois as regulações são muito menores e as variações são muito maiores – ampliando as possibilidades de ganho.

Os derivativos e *margin trade* são jogos de soma zero entre as contrapartes. Com os custos de transação, são jogos de soma negativa. Evite depositar valores significativos em qualquer corretora e depositar qualquer valor em corretora sem reputação.

Alavancagem é apenas indicada quando não tem liquidação forçada ou contra carteira diversificada, com a devida gestão de risco.

Estratégias com 100% de *TRACK RECORD* positivo até 2020:

Há estratégias com 100% de *track record* positivo em BTC e USD, tais como:

- Respeitar o múltiplo de *Mayer*, comprando abaixo de 200mma e vendendo acima de 2x200mma (Análise técnica);
- Comprar quando o *Google trends* indicar que expressões como *bitcoin* e *buy bitcoin* caíram abaixo de 50% da média e vender quando superarem 80%. Operar inversamente à manchete da CNBC teve 98% de acerto (Análise de sentimento);
- Comprar quando *hashrate* e número de transações por dia subirem sistematicamente e vender quando caírem (Análise fundamentalista).

4) Empréstimos p2p (*loan peer to peer*) e colateralizados

There is a war going on for ***your*** *bitcoins, and willpower is* ***your only defense****. Endless* ***Scammers*** *Everywhere. Bitcoin is a dangerous place.*

Os empréstimos pessoais (*p2p*) sem intermediação por empresa de crédito se iniciaram em plataformas como *btcjam*, *bitbond* e *bitlending club* em mercados insustentáveis (sem desenvolvimento de reputação entre partes) e colapsaram devido à ausência de colateral.

Empréstimos pessoais só são viáveis com *escrow* de confiança ou entre parentes: por exemplo pagando 2 ou 3x a sua mãe, avó ou tia o rendimento que ela tira no banco na perda fixa, dando a ela os bitcoins adquiridos como colateral.

O empréstimo de *fiat* colateralizado[348] em bitcoin é uma forma de consolidar renda em *USD/BRL* obtendo rendimentos superiores ao CDI, financiando a aquisição de bitcoins por juros inferiores aos cobrados pelos bancos pelo devedor.

Normalmente, quem contrai o empréstimo tem renda em *fiat* e deseja alavancar na aquisição de bitcoins, digamos, pegando R$ 200.000 emprestados a 2% ao mês. Se depois de 10 meses o preço do bitcoin aumentou 100%, o seu lucro na verdade foi 4000%, sendo que só pagou R$ 40.000 de juros e lucrou R$ 200.000.

Quem tem expectativa de hiperinflação em *rogue states*, Estados falidos, cada vez mais comuns, tem grandes resultados e motivações para alavancar em moedas locais. O ideal, muitas vezes, é obter alavancagem em fundos subsidiados (como venda de imóveis entre parentes, ou *lease back*).

Plataformas diversas como *Salt*, *Ethlend*, *Nexo.io*, *Celcius.network*, *Crypto.com, Binance, Blockfi e HodlHodl* também permitem empréstimos de dólares lastreados em criptos (e vice-versa), permitindo alavancagem.

A grande vantagem dessa operação é a elisão fiscal, uma vez que não há venda, não havendo fato gerador de imposto de renda, embora o investidor tenha acesso a dólares ou reais para pagar suas contas. A grande desvantagem é o risco de liquidação involuntária (*rekt*) se e quando o ativo dado como garantia (colateral) despencar de valor, abaixo do valor da dívida.

Negociar com empréstimos de bitcoins é altamente indicado para quem já tem experiência fazendo empréstimos e cobranças – especialmente com colateral e com pessoas com reputação, além das *DeFi*s (*decentralized finance*) e *CeFi*s (*centralized finance*).

Empréstimos colateralizados de *fiats* inferiores (como bolívar, peso argentino e real brasileiro) contra carteiras diversificadas (de bitcoins, com ouro, dólares e índices sintéticos de bitcoin, como DAI do *MakerDAO*) permitirão *bitcoiners (bitcoinheiros)* viverem perpetuamente como reis, comprando avião, iate e o que quiser sem pagar qualquer imposto de renda nem precisar comprar residência em Zug nem passaporte de St. Kitts, Vanuatu ou Antígua - porque empréstimo não é renda nem constitui ganho de capital.

Por isso se diz que logo você nunca precisará vender bitcoin, ele será como um título nobiliárquico que só é vendido quando a família já não tem mais nada.

5) Aluguel para margem (*lending for margin trade*)

Consiste em locação (*lending*) com intermediação por corretora (como *bitfinex*, *okcoin*, *blockfi*, *earn* e *poloniex*) ou para *traders* operarem *long* ou *short* – exatamente como aluguel de ações.[349]

Os saldos dos locatários são colaterais para pagamento dos locadores, havendo apenas risco de quebra ou incapacidade de execução da corretora.

Negociar com locação de bitcoins é indicado para quem pretende retornos entre 0,3% e 2% ao mês, suportando risco de custódia (insolvência das corretoras). Em especial, para quem buscar remuneração em *fiat* superior à das instituições de crédito convencionais e para quem pretende manter parte da carteira em *fiat* e parte em *cripto.*

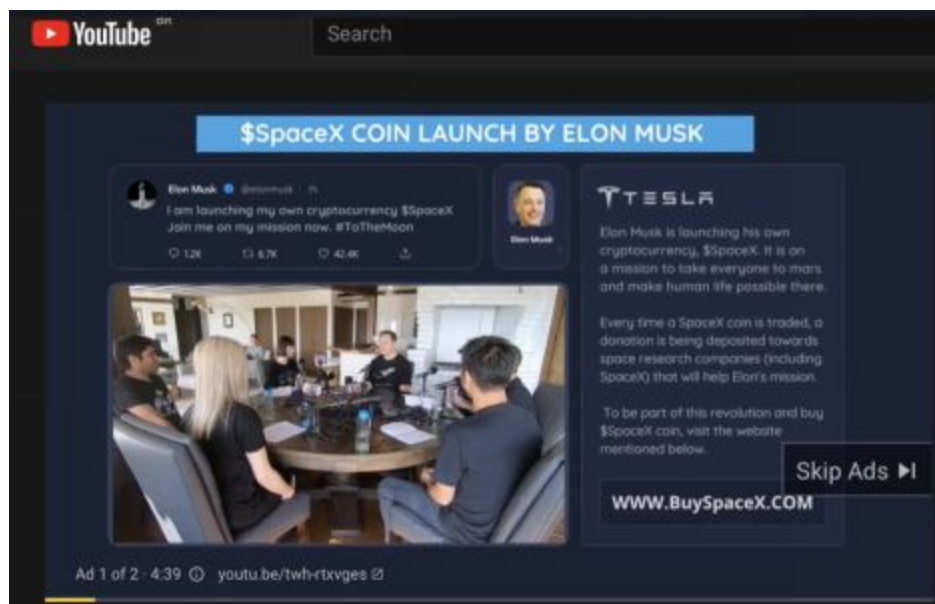
A utilização de *bots* (*software agents*) é muito comum tanto em *trades* quanto em *books* de aluguel. Em ambos os casos, recomenda-se leitura e estudo do seu funcionamento antes de colocar qualquer valor significativo. Se não forem usados *bots*, o aluguel pode demandar atenção diária para ajustar as ordens – altas o suficiente para dar algum retorno, mas baixas o suficiente para serem aceitas, não ficando com recursos parados.

Em geral, esse mercado gera diversas medidas relevantes. Quando o bitcoin está em tendência de queda, tende a ter remunerações maiores de aluguel; quando o bitcoin está em tendência de alta, geralmente a taxa para aluguel de bitcoin é mais baixa (e para aluguel de USD é mais alta).

Métricas[350] de mercado para medir otimismo são o *open interest* (total de contratos de derivativos em aberto que não foram liquidados); o percentual de ganho anualizado em fazer trava de bitcoin no mercado futuro (comprar bitcoin no mercado *spot*, presente; e, em sequência, vender futuro recebendo a diferença marginal como juro, remunerado em USD, ou vice-versa); e proporção de *shorts* e *longs* (indicando pessimismo ou otimismo).

Lending de *fiat* ou *stable fiat* (USDT, USDC, BUSD, por exemplo) também é uma forma de aumentar os saldos de quem precisa pagar obrigações nessas moedas, fazer *hedge* ou, simplesmente, “passar a chuva” esperando um momento de queda do bitcoin para recompra.

6) Pirâmides e *scams*, contos de fraudes

"Se você vê fraude e não diz fraude, você é uma fraude." - Taleb

Pirâmides são esquemas de remuneração de investidores pelo investimento de novos ingressantes, até colapsar quando não houver novos investidores suficientes, como a previdência obrigatória e insustentável de governo, como já foi demonstrado.

Casos famosos na comunidade brasileira de esquemas como este: *Anubis Trade*, *Atlas Quantum*, *Bitcoin Banco* (GBB), *Unick Forex*, *Dreams Digger Corporation* e vários outros.

Scam é uma expressão mais ampla que se refere genericamente à expropriação através de estelionato, até mesmo com *ICO* (*initial coin offering)* de criptomoedas inexistentes ou que não entregaram as funcionalidades anunciadas.

O mais comum atualmente é o pedido de depósitos justificados por hipotéticos *giveaway*: tipo, mande 1 bitcoin que vai ganhar 10, usando perfis *fakes* em redes sociais e impersonificação no *YouTube e até com contas oficiais do Twitter de personalidades como Obama, Biden, Musk e Buffet sendo hackeadas*[351].

Phishing é outra modalidade muito comum, em que domínios semelhantes a plataformas legítimas são criados e usuários que erram a digitação, ou os acessam por links anunciados em motores de busca ou mala direta, são induzidos a depositar saldos ou inserir senhas que deem acessos a saldos em sites de estelionatários. Isso também ocorre em sites de bancos e financeiras do *legacy* e demonstra que a cultura da criptografia e segurança da informação é, cada vez mais, essencial.

Outro golpe que chama a atenção pela ousadia e próximo ao *phishing* é a oferta de “falsas *wallets*” para *desktop* e *smartphones*, às vezes colocando até mesmo nas lojas oficiais de aplicativos os *softwares* falsos de estelionatários com nomes, símbolos, cores e tipografia semelhantes a produtos legítimos. Os incautos que não prestarem atenção e baixarem os referidos *apps* perderão os valores depositados, vez que acabarão por

revelar a *seed phrase* aos golpistas ou por criar carteiras a cujas chaves privadas eles já têm acesso.

Uma variedade de *scam* é o *exit scam* no qual os controladores das corretoras ou empresas fazendo custódia dos bitcoins simplesmente somem com os fundos dos clientes – normalmente, alegando que foram *hackeados* por terceiros desconhecidos e, em alguns casos, até simulando a própria morte (como alegado no caso da *exchange* canadense QuadrigaCX).

Há diversos golpes relacionados à manipulação de mercado, como divulgação de notícias e informações falsas ou sua manipulação (através de ataques de *spam* na rede aumentando *fees* e tempo de transações, ataques de *DDoS* tirando plataformas do ar); ou até mesmo por manipulação de preço para provocar liquidações involuntárias, para provocar *FUD* (*fear, uncertainty and doubt*) ou *FOMO* (*fear of missing out*); ou ambos, como nos esquemas de *pump and dump* que justificam a maioria dos grupos de "*calls* para trade", no *Telegram*.

Quem compreende que retornos são proporcionais a esforços e riscos compreende que promessas de retorno garantido "perpétuo de 3% ao dia" ou de "dobrar seus bitcoins semanalmente" claramente são mentiras e indicam evidências de crime.

Muitas pessoas têm seu primeiro contato com bitcoin caindo em golpes – e, na maioria das vezes, tornam-se *haters* depois do *rage quit,* porque a única maneira de reduzir a sua culpa e automartírio por causa da ingenuidade e perda de oportunidade é o bitcoin "morrendo". Isso ocorre devido às propriedades úteis do bitcoin, como relativa anonimidade. Pessoas livres aprendem com a experiência, perdedores culpam as sombras.

7) *Ransomware* (sequestro de dados)

> As maiores mentes do mundo estão no Bitcoin, as maiores mentes criminosas também.

Consiste em espécie de *malware* que, após infectar o sistema, cobra "resgate" para que o acesso seja restabelecido. Em empresas com conteúdo de recuperação impossível ou inviável – como escritórios de advocacia –, muitas vezes a decisão de pagar a chantagem é inevitável[352].

Um caso de *ransomware* que popularizou o bitcoin foi o *wannacry*[353] em 2017. Diversos órgãos de inteligência acusaram que esse *malware* era um ataque norte-coreano[354]. Mesmo após a divulgação pública de que o pagamento não fazia os criminosos liberarem os dados, o golpe arrecadou mais de 50 bitcoins em 2017 (e continua arrecadando, como se pode conferir em seus endereços).

Muitas vezes, mesmo pagando o resgate, o código de desencriptação necessário para acessar os arquivos não são enviados. Esta possibilidade deve ser considerada na decisão sobre pagar ou não aos criminosos.

8) Arbitragem entre *exchanges* e moedas

Arbitragem é a operação praticamente simultânea em diferentes mercados, com obtenção de lucro, em teoria, sem risco, embora na prática existam riscos de *slippage* (diferença entre preço esperado e real, muitas vezes devido a sua própria ação em ordens ativas mudando cotação) e de solvência das plataformas (risco de custódia), como qualquer operação em plataformas centralizadas ou descentralizadas.

Arbitragem entre *exchanges* (corretoras) é possível quando são identificadas diferenças de valor que compensem os custos de transação. Como a mineração é inviável no Brasil, pode-se supor que quase todos os bitcoins em circulação foram "importados" por este processo.

As diferenças de preço (*spread*) entre corretoras de outros países apresentam variações ainda maiores. Assim, o ágio (*spread*) indica a dificuldade de fazer remessas internacionais. Nesses casos, lucra quem pode fazer envios internacionais com baixo custo – seja usando plataformas como *Zro Bank*, *Wise (antiga TransferWise)* ou remessaonline.com.br, seja levando dinheiro fisicamente ou tendo facilidades, como as oferecidas pelo BB Americas, XP investimentos ou outros bancos comerciais a alguns clientes.

Caso a compra e a venda não ocorram simultaneamente, há o risco de "*slippage*" – que a variação na cotação destrua a margem de lucro. O ágio do bitcoin no Brasil tem caído sistematicamente, reflexo da base consumidora deste mercado, que tem aumentado exponencialmente.

9) *Bounties* e novos serviços

“Novos serviços no ecossistema” podem ser: suporte operacional, técnico ou de desenvolvimento, como colaborador independente: *Bitrefill*, bitmilhas, p2p. Advogados, contadores, designers, programadores especializados são altamente demandados.

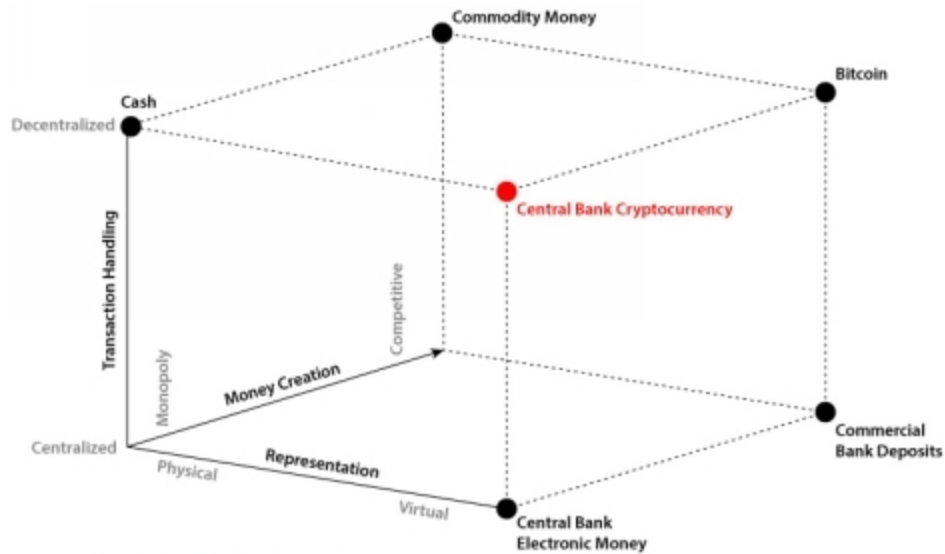
Depois que o ecossistema atingir certa massa crítica, as pessoas que não tiverem as habilidades para utilizá-lo ficarão obsoletas. Pode ser desenvolvendo aplicativos ou comprando e vendendo bitcoin na vizinhança usando *network* orgânico ou na gestão de redes sociais, a demanda por estes profissionais é maior que a oferta.

As habilidades necessárias para oferecer serviços no ambiente dependem de educação real – que é o oposto ao que é oferecido na instrução formal – e isso demanda assunção de riscos e esforços.

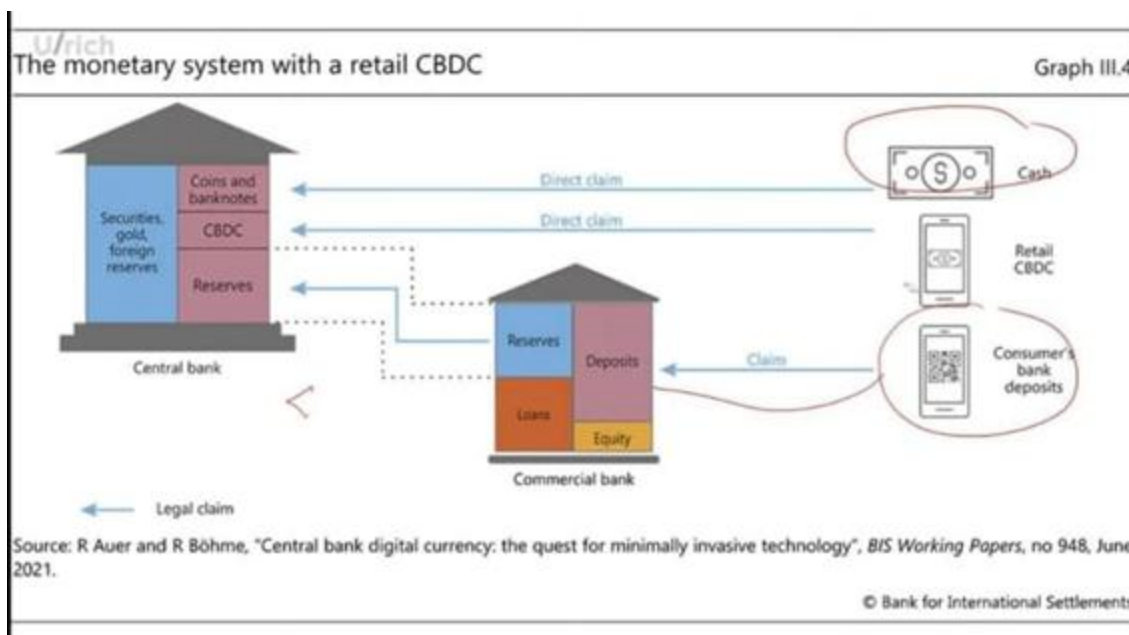
Bounty é espólio, butim, normalmente prêmio feito como: divulgação por *referrals* de indicação de inscrição em plataformas, remuneração de c*ommunity managers* (com serviço de suporte, produção de vídeos e divulgação em redes sociais), a descoberta ou correção de *bugs* e falhas de segurança em plataformas e até em *blockchains.*

9.1) O novo serviço problema: CBDC’s

Os bancos atualmente são a antítese do capitalismo. A deterioração do *Deutsche Bank* e do sistema bancário europeu é evidência do esquema insustentável a que são submetidos. A sua chance de sobrevida virá da “Guerra ao dinheiro”, das tentativas de limitar ou eliminar o dinheiro físico (implantando o controle totalitário sobre as finanças), como nas CBDCs[355].

Figure 1: Control Structure of Currencies
NOTE: Figure 1 is adapted from Berentsen and Schär (2017).

As CBDCs[356] não são semelhantes a criptomoedas, são seu exato oposto: totalmente centralizadas, vulneráveis a expropriações voluntárias, violações de privacidade, mudanças de regras sem consenso; e, a diluição por senhoriagem[357]:

As CBDCs – *Central Bank Digital Currencies* (moeda digital de Banco Central) aumentam brutalmente o poder dos governos, inclusive sobre os bancos, uma vez que o próprio banco central vai processar as transações (como no PIX) e manter registros de todos os saldos. Estudos da ONU e do FED indicam que as CBDC’s poderiam matar os bancos comerciais e que a próxima etapa da “*FED Coins*" seria o “*FED APP"*, dispensando a intermediação bancária[358].

O fim dos bancos como conhecemos:[359]

Quanto mais agressivas forem as tentativas de expropriação de bens[360], imposição de sistemas de créditos sociais para acesso a negócios ou serviços; e, criminalização/restrição de atividades econômicas negras e cinzas[361], maior será a demanda por alternativas.

Como vão operar camelôs, indigentes, traficantes, profissionais de saúde que operam sem recibo, GPs, políticos comprando votos e o jogo do bicho - apenas como exemplos rotineiros - com o fim da moeda alodial? Vão pagar no PIX? Vão voltar a usar ouro e prata? Ou vão desistir das atividades informais e ilegais? Você tem as ferramentas e conhecimento para certificar a pureza de ouro ou prata? Acredita que a banca de jogo do bicho terá?

9.2) As soluções: uberização e empreendedorismo

Uberização é o processo de criação de valor em intermediação provendo ambiente negocial com algum grau de segurança entre partes, oferecendo plataforma em que serviços e produtos são ofertados e aceitos com sistemas de reputação e *escrow* - como *Uber, Airbnb, iFood, Silk Road* e *Bisq.*

Dezenas de bilhões de dólares estão sendo investidos em *FinTechs* (como *Circle, Uphold*, *Bitpay* e as diversas empresas mencionadas). Os bancos e demais instituições financeiras não têm expectativas positivas com juros sistematicamente negativos e crescente competição de serviços que não estão submetidos a suas regulações extremas.

Não foram apenas entes de reputação e legado superiores, como Satoshi, que ficaram bilionários empreendendo no ecossistema, também há figuras abjetas como Vitalik (*Ethereum*) e Roger Ver (*Bitcoin Cash*), além de outras controversas - como Changpeng Zhao (*Binance*), Sam Bankman-Fried (*FTX*) e os irmãos Winklevoss (*Gemini-Blockfi*) nesse *ranking*. Um exemplo de empreendedor controverso (já preso, inclusive) que produz conteúdos de altíssima qualidade é o Arthur Hayes, da *Bitmex*[362].

As oportunidades são amplas e a disponibilidade de investimentos por *private equity* e *venture capital* é crescente.

Os riscos do pioneirismo são altíssimos. Centenas de *altcoins* viraram pó, não tendo mais negociação em qualquer corretora. Várias empresas no ecossistema foram *hackeadas* e faliram.

A infraestrutura básica mudou em cada Era:

1) (2009-2012): repositórios para *download*, fóruns, *faucets, exchanges* estáticas[363], *mineração com GPU/FPGA e* apostas simples aleatórias, com oráculo *onchain*, como *satoshidice*[364];

2) (2012-2016): corretoras com *fiat, stables* e *margin trade, sites* de notícias e relatórios especializados, plataformas de apostas multilaterais de eventos como bitbet.us, *ATM*s de BTC e mineração com *ASICs*;

3) (2016-2020): *DeFis, exchanges* com sintéticos (negociando futuros e derivativos, como *Bitmex* e *Deribit*), plataformas de empréstimos colateralizados (viabilizando consumo legal sem imposto de renda e alavancagem, como *Nexo*, *Blockfi* e C*elcius*), de trocas *offchain* (saldos entre clientes) e 2ª camada (*Lightning*), *Sidecahins*, *DLCs* e *gateways* alternativos (cartões pré-pagos e *marketplaces* de milhas e *gift cards*), *air-gapped hardware wallets* (carteiras *offline* sem contato físico com terminais)[365].

4) (2020-2024) *ETF*s e fundos de BTC, facilitando acesso institucional sem risco de custódia, plataformas de serviços financeiros completos - que além de *margin trade*, opções e futuros, ofereçam colateralizados contra carteiras múltiplas, *copy trade* substituindo "gestor profissional", capitalização passiva de saldos com *bot* alocando em *cash and carry*, *lending* ou empréstimo; e, tokenização de índices, ações, moedas e *commodities* (sintéticos colateralizados em BTC ou lastreados em saldos da plataforma) que possam ser negociados 24/7 (tornando corretoras convencionais de ações obsoletas); e, tokenização de apostas de eventos negociadas em *books* como os *tokens* TRUMP2020, TRUMP2024 ou BOLSONARO2022[366] na *FTX*. *Wallets* que integrem funções de *chat* com transações em diversas camadas - como a *Zebedee* com *Discord, Status, Alipay e WeChat*. Plataformas de *podcast* com remuneração direta aos produtores de conteúdo via soluções de segunda camada, como *Breeze* e *Sphinx*.

5) Na 5º Era (2024-2028), a tendência é que as *wallets* interajam além de transações em várias camadas e serviços de *chat*, oferendo outros serviços de comunicação e privacidade (como *VPN*, compartilhamento remunerado de banda, capitalização e colateralizado sem intermediários e oferta ou aceitação de serviços e produtos "uberizados"). Neste período, as plataformas

> sobreviventes devem ampliar os serviços oferecidos e, após substituir bancos e corretoras de valores, passem a substituir também loterias, seguradoras e, finalmente, a justiça estatal com serviços de apostas decentralizadas de morte e decisões decentralizadas de conflitos[367].

Durante as 4ª e 5ª Eras será esperado que a maioria das corretoras que dependam de serviços bancários em países bolivarianos sejam eliminadas (criminalizadas ou inviabilizadas por regulamentações) ou capturadas (adquiridas por cantilionários amigos do rei). O sistema bancário convencional será brutalmente impactado por *CBDCs* e *APPs* de bancos centrais, até mais do que já sofreu na última década com as *fintechs* e o juro negativo. Após os Bancos Centrais serem responsáveis por processar a maioria das transações (como no PIX), eles tenderão a oferecer plataforma oficial para pagamentos e capitalização (estatal ou de empresa com controladores ligados intimamente a governo[368]), eliminando a necessidade de intermediários bancários – facilitando ainda mais a manutenção de juros reais negativos.

Cada etapa dessa guerra apresentará novas e enormes oportunidades aos emprendedores.

Hal Finney
*"**Running Bitcoin**"*
(Twitter)

Arte de comemoração ao 10º aniversário de Hal Finney *'Running Bitcoin'*.
(10 de jan de 2009) / **Fonte:** Cryptograffiti (artist)

Roteiro passo a passo para comunidade *bitcoiner*:

1) Estude, com ceticismo, *Twitter*, *Bitcointalk*, *Discord*, *GitHub e Reddit*, que são os lugares onde se concentram as principais discussões *crypto*[369]. A maioria das comunidades abertas do Facebook e propagandas do YouTube são antros de criminosos ou pura desinformação. Acompanhe os *meet ups* locais.

2) Cadastre-se nas plataformas nacionais (*Walltime*, *Rispar*, *Foxbit*, *Biscoint*, *Bipa.app*), pesquise quem vende ou compra a melhor preço no biscoint.io antes do depósito e não venda mais de

R$ 35 mil por mês por CPF em corretoras nacionais, se não quiser pagar imposto;

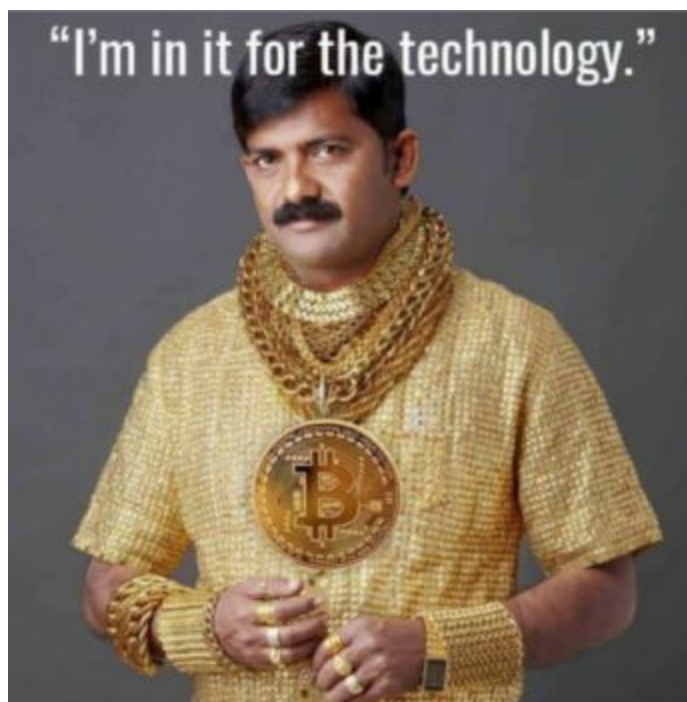
3) Acompanhe as comunidades internacionais (*reddit*, *bitcointalk*, IRC WOT); e os canais do *YouTube* e livros de "evangelistas" como Bitcoinheiros, Andreas Antonopoulos e Saifedean Ammous; e podcasts, como Stephan Livera e Jimmy Song;

4) Abra conta nas corretoras estrangeiras com reputação e tenha intimidade em usar plataformas — fornecendo apenas *email* de *small tech*[370] que valorize privacidade e não exija dados pessoais. Nunca use para nada de relevante *e-mail* de *big tech*. Essas podem fornecer *master keys* a governos totalitários e policialescos[371] e usar seus dados para reduzir seu “extremismo” usando técnicas de “desradicalização”[372] por *nudging*;

5) *Exchange* (corretora) não é carteira. Utilize para guardar seus bitcoins apenas soluções como *paper wallets* geradas *off-line* e criptografadas, com *passphrase* (para os mais avançados); *Wallet mobile* (para pequenas quantias e de preferência que use *Lightning Network*); e *Hardware wallets* (para uso constante, sem depender de uso de navegadores, com recursos como *multisig*);

6) Utilize, após referências e pesquisas, demais empresas e serviços do ecossistema – *Fold*, *Bitrefill*, *Glin*, *Celsius network*, *NEXO*, *BlockFi*, *Crypto.com*, *Hodlhodl*, *LocalBitcoins e* opções descentralizadas como a *Bisq*;

7) Seja feliz com sua independência.

O que foi mencionado até aqui é o presente e o básico, agora se quiser aprofundar e vislumbrar o futuro, continue.

Bitcoin Memes – "Estou aqui pela tecnologia."

CAPÍTULO III:
PERSPECTIVAS FUTURAS E AMEAÇAS

1) É bolha?

É importante refutar o mito repetido de que “bitcoin é bolha”. Na verdade, o bitcoin é a agulha que pode estourar “a bolha de tudo”[373] (*the everything bubble*) criada pelo juro negativo, com governos comprando trilhões em ativos a qualquer preço e mantendo vivas empresas zumbis (cujo faturamento é insuficiente para pagar os juros das dívidas).

Robert Schiller, prêmio Nobel e docente de um curso gratuito de finanças no *Coursera*[374], nas edições mais recentes de seu livro *Irrational Exuberance*, afirma que “o maior exemplo de bolha da atualidade é o bitcoin”.

Bolha econômica ou de ativos, bolha de mercado, bolha especulativa ou bolha financeira são sinônimos e descrevem a situação em que o preço de um ativo se descola do seu valor fundamental. Um critério objetivo para a sua definição é quando o preço de um ativo sobe mais que dois desvios-padrão.

Isso ocorre ciclicamente no BTC, devido aos processos de *FOMO* (*fear of missing out*), normalmente no ano imediatamente posterior a cada *halving*, logo depois corrigindo (também seguindo padrão emocional, *FUD* (*fear uncertainty and doubt*) para recomeçar o ciclo. Como o Bitcoin tem fractal próprio, em decorrência dos choques de oferta nos *halvenings*, ele ciclicamente entra em “bolha” quando seus retornos médios ultrapassam o dobro do seu desvio-padrão.

Adotando a definição de bolha baseada em análise técnica (bolha a partir da variação superior a dois desvios-padrão), o bitcoin passou por quatro bolhas: 1) de abril até junho de 2011, de 0,31 para 31 USD; 2) entre dezembro de 2012 e abril de 2013, de 13 para 266 USD (Crise cambial do Chipre); 3) de junho a novembro de 2013, de 100 para 1.300 USD; e 4) de abril a dezembro de 2017, indo de 1.200 até 19.700 USD[375].

Em cada uma dessas oportunidades, nas quais multiplicou de valor 100x, 20,5x, 13x e 14,91x, existiram correções equivalentes e subsequentes

períodos de acumulação – exatamente como previsto na Teoria das Ondas (de Dow e Elliot) e nos seus “Ciclos emocionais de mercado”.

O preço do bitcoin passou por bolhas e tende a passar por outras mais, quando seu preço aumentar mais de 10x em poucos meses. Porém, em sua tendência normal de aumentar no ritmo do aumento de sua base de usuários, não se pode afirmar que seja bolha, mas apenas consequência da Lei de Metcalfe[376] e curva normal de adoção de tecnologia, a não ser que razões políticas ou técnicas indiquem perda de valor fundamental.

Em termos fundamentais, bolha é quando o preço descola dos seus parâmetros de precificação.

Razões políticas podem mitigar o valor fundamental do Bitcoin. Se os principais governos mundiais voltarem ao padrão-ouro com conversibilidade integral, se os principais governos do mundo funcionarem em superávit (arrecadando mais do que gastam), se forem revogados todos os controles de capitais, tributos e expropriações involuntárias, assim como as limitações para o comércio e o investimento globais, aí, sim, o Bitcoin poderá perder grande parte de seu sentido, sua base de usuários e seu valor fundamental.

Interessante notar que as experiências de proibição e criminalização das operações com criptomoedas não resultam em redução do seu valor na respectiva jurisdição – pelo contrário, exatamente como a proibição das drogas ou do álcool, passa a haver ágio.

Razões técnicas também podem mitigar o valor fundamental do Bitcoin, tais como: 1) se houver queda significativa do *hashrate*; 2) se uma quantidade significativa de desenvolvedores abandonarem o projeto (ou forem presos ou mortos); 3) se uma quantidade significativa de *tokens* for apropriada por entidade disposta a vender por qualquer preço, como aconteceu com a massa falida do *Mt. Gox* e a *Tokyo Whale*; ou 4) se o sistema sofrer ataques significantes, como os ataques de *spam* dos mineradores em 2017, que encareceram as *fees*.

Até que ocorra o fim (ou irrelevância) dos governos como conhecemos, é crível que as razões políticas venham a mitigar o valor do Bitcoin.

Bitcoin Memes

> "A questão não é quanto alto pode ir o Bitcoin, mas, sim, quão baixo pode ir o dólar. Se o dólar for a zero, o valor relativo do bitcoin será infinito…"

1.1) Qual o valor de uso do bitcoin?

Serve para fazer remessas internacionais independentemente de controles de capitais, para garantir imunidade contra tributos e execuções involuntárias em face de ditaduras e perseguições institucionais, e serve como reserva de valor pseudoanônima imune a diluição de moedas e de políticas governamentais.

Quanto maiores os tributos, quanto mais absurdas as regulações, quanto maior o *déficit* e maior a dívida pública, quanto mais numerosos forem os embargos e controles de capitais – mais útil será o Bitcoin.

É uma hipótese plausível e corrente na comunidade que, se os governos tivessem mantido o padrão-ouro, com conversibilidade integral, o tamanho dos Estados teria permanecido limitado; e, provavelmente, o Bitcoin nunca teria sido criado; e, se fosse, não teria se popularizado.

Dessa forma, o Bitcoin foi criado em decorrência do abuso de poder e corrupção extrema dos governos – como repetidamente confirmado por Satoshi até mesmo no Bloco Gênese ao escrever o texto *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*. Assim, quanto maior o descontrole e o abuso governamental, maior deve ser o valor fundamental do Bitcoin.

The Times de 3 de janeiro de 2009. O Bloco Gênese deixou uma mensagem, a qual faz referência a esse jornal. Atualmente, um exemplar dessa edição vale milhares de dólares e é objeto colecionável.

THE TIMES

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen
Frost, Nixon and me

Working mums
So that's how she does it

Detox in style
The best spas on the planet

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Salman Rushdie
I won't marry again

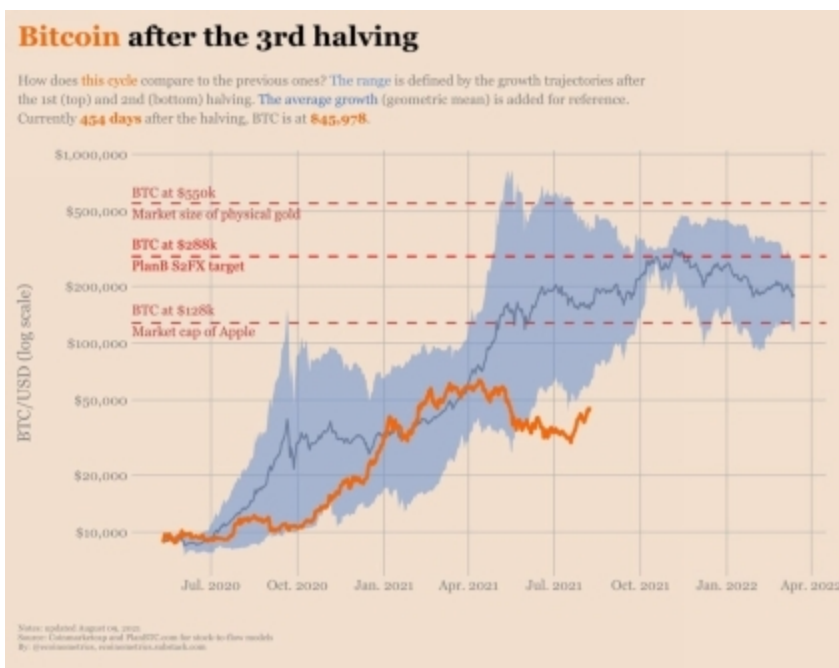
Giant killing?
Guide to the FA Cup third round

O valor das dívidas corporativas globais é exponencial, assim como as limitações quanto às liberdades individuais e a ampla consciência de que o sistema em que vivemos é inevitável – como popularizado por Peter Schiff e Mike Maloney, além de outros expoentes da Escola Austríaca. É isso que alimenta a tendência exponencial, desde 2010, do valor do bitcoin.

A primeira definição é mais complexa de classificar, pois o valor fundamental do Bitcoin (como de qualquer criptomoeda) é subjetivo e depende de obtenção de dados estimados (e não objetivamente calculados), como número de usuários, velocidade de circulação, *proof of brain* (captação relativa de cérebros), *proof of stake* (captação de investidores relevantes), *proof of work* (capacidade computacional dedicada) e até mesmo a qualidade das contribuições no seu repositório e das empresas no seu ecossistema – há uma série de artigos de alta complexidade sobre o tema.

No canal Aimstone do *YouTube*, há um episódio de 2018 muito didático explicando a estimativa de US$ 1,2 milhão por bitcoin como valor alvo, por uma lógica simples: nos anos anteriores, o aumento no número de carteiras era proporcional ao aumento de preço (ambos multiplicaram 20x); então, assumindo como limite de crescimento algo em torno de 2,4 bilhões de usuários (todas as pessoas entre 18-64 anos com acesso à *Internet* e a *smartphones*) o aumento dos atuais 20 milhões para 2,4 bilhões de pessoas ocorreria, seguindo a taxa atual de adoção, em 4 a 7 anos. No mesmo canal, a estimativa mais atual[377] é de US$ 12,5 milhões de dólares por bitcoin em 2031.

Valuations lineares são comuns, até mesmo no relatório de Ray Dalio, existem as estimativas de preço para os cenários que o bitcoin ficaria com x% do mercado do ouro, y% dos mercados de remessas e z% dos mercados de ações e imóveis. O problema com essas estimativas é que a base de cálculo (riqueza mundial) não é estanque, de modo que, quanto mais pessoas adquirem o bitcoin, mais riqueza é gerada com mais liberdade econômica e menos riqueza é destruída por distorções derivadas do juro negativo e totalitarismo.

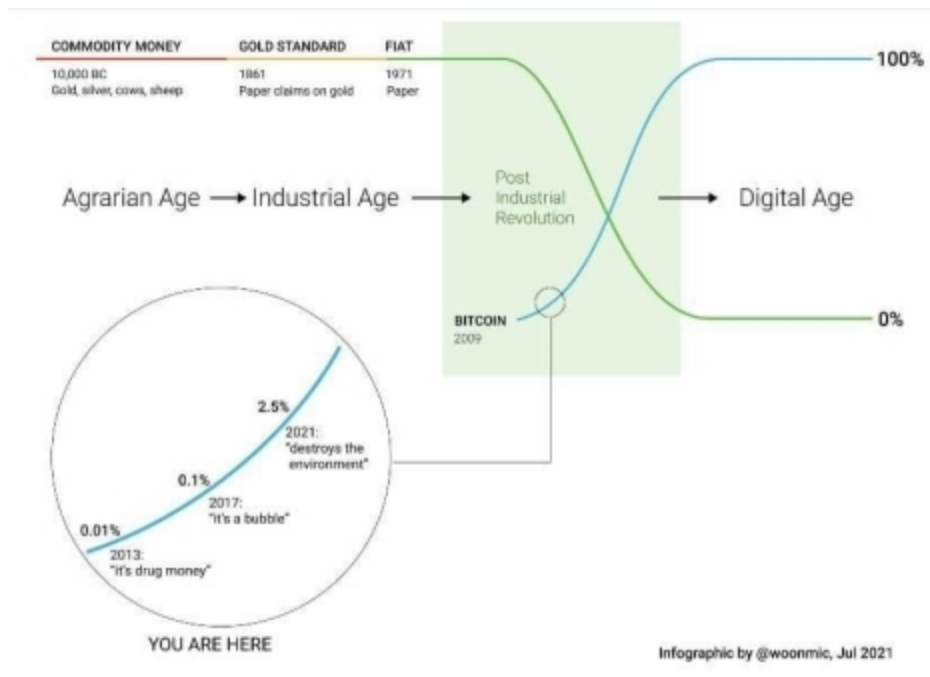
Dizer que o bitcoin precisa valer valer 550k USD para bater o *market cap*[378] do ouro não diz muito, até porque há quem[379] defenda que XAU (31,1 g) pode valer US$ 50 mil em 2022, com a volta do *gold standard:*

A questão é um pouco mais complexa, pois estão sendo desenvolvidos produtos financeiros que permitam a instituições investirem em bitcoin sem o risco de custódia, com destaque para *Fidelity, Grayscale, Purpose e Bakkt*. Como a maior parte dos recursos nos mercados pertencem a instituições e não a pessoas físicas, a projeção mencionada já perde o sentido.

Se o BTC avançar segundo as cinco fases de Barry Silbert[380], a quarta fase (atual) é a adoção institucional (compra por corporações fundos e investidores institucionais por meio de ETFs) e a próxima (5ª fase) será quando órgãos governamentais (Bancos Centrais) e supranacionais vão competir adquirindo bitcoin (primeiro como reserva, depois como lastro de moeda; e, por fim, como moeda) – seja comprando a mercado ou desapropriando bitcoins de seus cidadãos (como Andreas Antonopoulos teme que ocorra com eventual *ETF*). Outra maneira de governos acumularem bitcoins é parando de leiloar os bitcoins apreendidos – como o governo norte-americano faz constantemente.[381]

Para o venezuelano cuja alternativa à criptomoeda é acumular bolívares, que perdem metade do valor a cada 18 dias; para o trabalhador ilegal em países de economia desenvolvida, que precisa mandar recursos para sua família também desbancarizada no interior de jurisdições de economia subdesenvolvida; ou, para o empresário que quer pagar certa comissão

ilegal que, se for rastreada, resulta em cadeia (como Eike Batista foi preso), as criptomoedas podem ter valores utilitários peculiares.

Agregar as demandas mencionadas apenas em DeFi (protocolos de finanças alegadamente descentralizadas) é uma tarefa improvável. Os mercados descentralizados podem ser oferecidos por redes federadas (como *Liquid*) ou de 2ª camada (como *Lightning*) de maneira mais barata, rápida e segura que *blockchains* marginais. Talvez o mercado de *smart contracts* seja perpetuamente algo de nicho e talvez substitua grande parte do mercado CeFi (financas centralizadas), em todo caso, a participação do bitcoin nesses mercados tende a ser crescente com diversas atualizações aumentando sua fungibilidade, escalabilidade e funcionalidade, como o *Taproot (BIP341)* e posteriores:

Tendências de Migração das Riquezas

O ecossistema de criptomoedas mostra como funciona o livre mercado real. Mesmo com proliferação de crimes e manipulações — como aquelas relacionadas a emissão de USDT[382] (por inexistência de colateral ou colateral sem qualidade) e as decorrentes dos mercados futuros[383] na *CME/Bitmex/Deribit/LedgerX/Bakkt* para provocar "*maximum pain*[384]" nos mercados de opções — o mercado se autorregula de maneira anti-frágil, se aperfeiçoa pelo aprendizado e ninguém recebe *bail-out* mesmo com quedas de mais de 90% das cotações de mercado.

A liberdade suprema leva à responsabilidade extrema. No Bitcoin não há como mudar as regras no meio do jogo, como acontece no Ethereum.

Estimativas mais simples do valor fundamental do Bitcoin são feitas a partir da consideração de quanto dos mercados existentes ele pode ocupar – por exemplo, se o Bitcoin tomasse metade do mercado do ouro[385], valeria mais 6 trilhões em *market cap* (US$ 330 mil por bitcoin com ouro a US$ 1.900); se o bitcoin ocupasse 20% das *offshores* em paraísos fiscais, abocanharia mais 7 trilhões de dólares; e assim por diante, em mercados de remessas; *black* e *gray markets* (como tráfico de drogas, armas, escravos, corrupção e descaminho); e até os mercados de ações (US$ 120 trilhões), *fiats* (US$ 110 trilhões) imóveis (US$ 300 trilhões), dívidas (US$ 300 trilhões) e derivativos (entre 0,6 e 1 quadrilhão de dólares) que tendem a perder um percentual de seus investidores para o Bitcoin.

O PIB global foi de 88 trilhões de dólares em 2019 (mais que o dobro daquele de 1990). A criação e acumulo de riquezas são exponenciais – e só perdem para o ritmo atual de aumento de dívida e impressão de moedas fiduciárias.

Para se ter uma ideia do quão irrelevante ainda é o mercado de bitcoins (embora já tenha superado o *market cap* da prata), pode ser demonstrado que, segundo compilação da *visualcapitalist*[386], existiam mais de 2.100 indivíduos bilionários (com patrimônio médio de mais de 8 bilhões cada); mais de 13 milhões de *HNWI (High Net Worth Individuals*, com patrimônio líquido de mais de US$ 20 milhões); e, mais de 50 milhões de milionários (em patrimônio líquido em dólar). Isso era em 2020, agora é muito mais.

Assim, a riqueza privada formal do mundo é estimada em mais de um quadrilhão de dólares, se forem somados os ativos públicos e mercados negros e cinzas, deve ser muitas vezes mais.

Se as taxas de inflação do ouro[387] mantiverem sua tendência histórica[388], nunca haverá mais que 1 bitcoin para cada 10 quilos de ouro (199M kg/19M BTC > 0,1 BTC por kg). Retirando daí os bitcoins perdidos (já que as reservas de ouro não contam ouro no fundo do mar), seriam 12 a 13 kg de ouro por BTC[389] (em agosto de 2020 avaliados em mais de 4 milhões de reais).

Com o total de 8 bilhões de pessoas no mundo[390], seria: 21M/8B = 0,002625 BTC por pessoa; e, 21M/50M = 0,38 BTC por milionário. Isso considerando a emissão máxima final a ser atingida em 2140, se formos subtrair os milhões de bitcoins perdidos e milhões ainda não criados o valor ainda seria 30 a 45% menor. Se bitcoins ainda existirem em 12 anos, serão mais escassos que imóveis ou qualquer outra classe de ativo, como demonstrado no S2FX.

São emitidos apenas 900 novos bitcoins por dia, na Era atual[391]. É quase impossível que uma entidade (mesmo governamental) que comece a comprar agora consiga captar a mercado mais que os 654.885 sob custódia da Grayscale[392] ou que uma corporação acumule reservas[393] superiores a Microstrategy (105.085 BTC) e Tesla (38.300 BTC)[394], se os últimos não forem desapropriados ou venderem de maneira relevante.

Todo bitcoin tem um preço, mas a maioria deles não esta à venda por *fiat*, mas por liberdade – território soberano, passaportes com isenção perpetua de tributos e realização de sonhos.

Se mais de 86% não venderam seus bitcoins na queda, em 2018, de US$ 19.500 para menos de US$ 3.500, quantos venderão facilmente quando vier a hiperinflação em *fiats*? É a "minoria intransigente”de Taleb.

Revista Veja, dezembro de 2017.

NEGÓCIOS

Grupo Abril é vendido por R$ 100 mil para especialista em aquisição de empresas quebradas

Por R$ 100 mil, o empresário Fábio Carvalho comprou a Abril, assumindo os R$ 1,6 bilhão de dívidas que causaram o pedido de recuperação judicial

Em alguns anos, um exemplar destes valerá mais que a Veja (empresa com todos os ativos) em um leilão de colecionáveis. O grupo dono da VEJA foi vendida em 2018 por 100 mil reais - provando que "você pode ignorar a realidade, mas não as consequências dela".

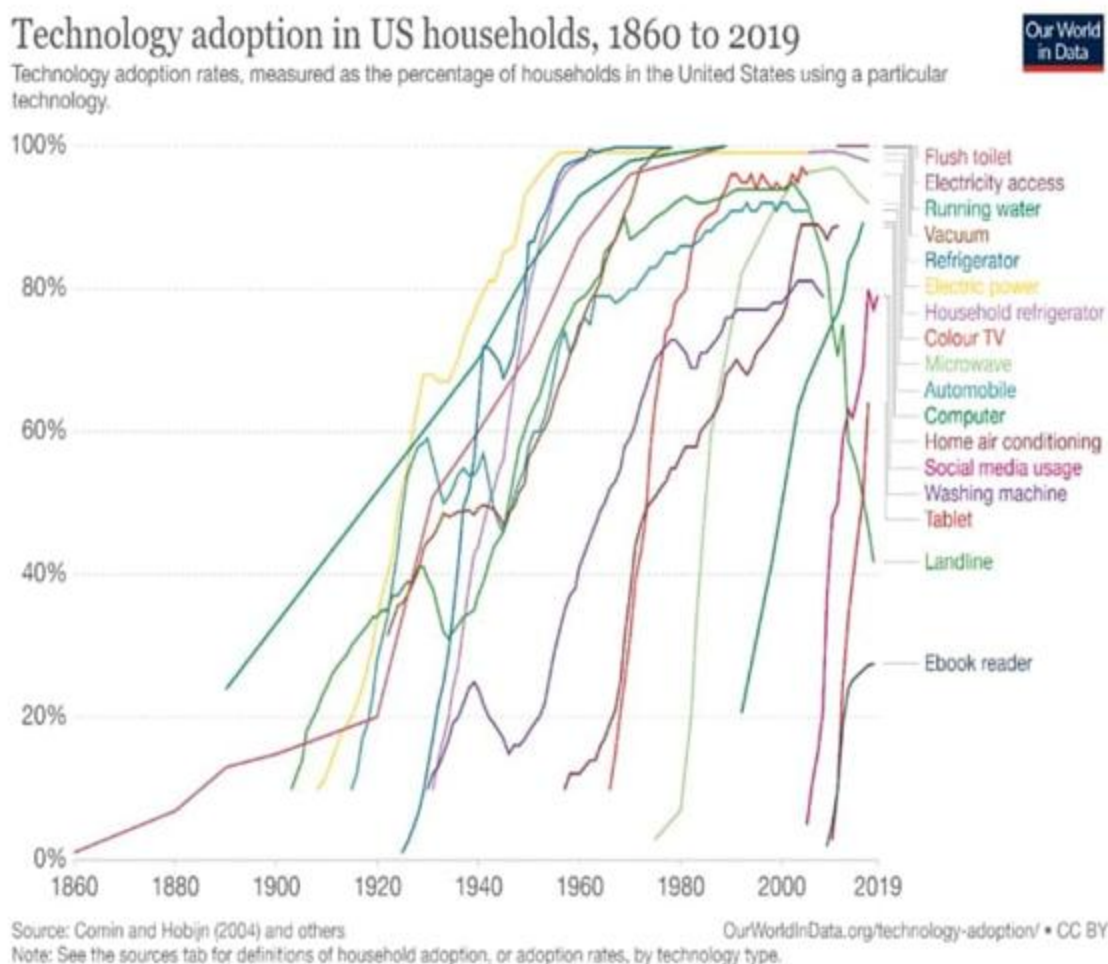
Uma coisa é certa: quando aprenderem a operar criptomoedas, nunca mais petistas precisarão viajar com dólares na cueca, nem amante de presidente levar dezenas de milhões de euros no avião presidencial, nem peemedebista baiano alugar apartamento para servir de depósito de dezenas de milhões de numerário em espécie; e, muito menos, senador bolsonarista vai precisar ser humilhado com a polícia tirando 30 mil reais de seu traseiro com resíduos de fezes (episódio que deu outra dimensão ao conceito de "dinheiro sujo"). Também neste aspecto, o Bitcoin é o dinheiro mais limpo já criado.

Se a população do planeta não for agressivamente destruída, nunca existirá nem 1 bitcoin para cada 420 pessoas. Por esses motivos, acredita-se que, no futuro, os preços serão expressos em satoshis, se o bitcoin atingir a fase 5.

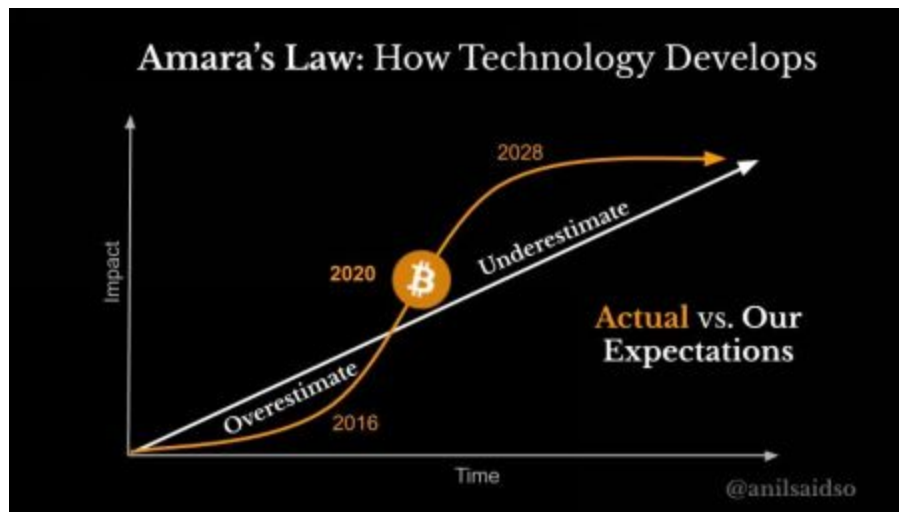
Há projeções que indicam que, se a taxa de adoção e o aumento de preços exponenciais forem mantidos, em 10 anos, as criptomoedas tenderão a sugar o valor hoje circulando em moeda fiduciária estatal (US$ 100 trilhões, em dezembro de 2019). Isso não será o fim das *fiats*, mas o fim de sua significância. Elas podem continuar existindo, como hoje existem as indústrias de selas e de lampiões – embora sejam objetos obsoletos.

A questão é que o bitcoin, ao valorizar 100x, cria riqueza e propicia negócios e eliminação de perdas como *malinvestments*, de modo a aumentar a riqueza total.

Existem dois porquês pelos quais o valor do bitcoin pode subir exponencialmente – ao contrário do valor de ações e de outros ativos limitados a fluxos de caixa de negócio ou bens físicos: 1) a Lei de Metcalfe enuncia que o valor de conexão em uma rede é proporcional ao quadrado do número de participantes: quanto mais pessoas tiverem bitcoin, mais fácil será encontrar pessoas que o negociem; quanto mais dinheiro for investido no ecossistema, dado que sua oferta é predeterminada e não pode ser inflacionada, maior o valor que o *token* poderá alcançar; e 2) sua oferta tem inflação decrescente, mesmo que a demanda seja constante, a sua oferta

marginal é decrescente – isso sem considerar os bitcoins perdidos – também em decorrência da Lei de Metcalfe, o valor de tecnologias adotadas geralmente aumenta de maneira exponencial até atingir um platô e estabilizar. O gráfico seguinte mostra a “curva S” para várias tecnologias:

Tendemos a superestimar o efeito de uma tecnologia no curto prazo e a subestimar seu efeito no longo prazo.

Roy Charles Amara

Este fenômeno é conhecido como Lei de Amara:

2) Ciclo de hype da tecnologia: Gartner Hype Cycle

O *Gartner Hype Cycle* é uma metodologia que oferece uma visão de como uma tecnologia ou aplicativo evoluirá ao longo do tempo, fornecendo uma fonte sólida de insights para gerenciar sua implantação dentro do contexto de seus objetivos de negócios específicos. O ciclo fornece uma representação gráfica da introdução, maturidade e aceitação de novas tecnologias.

De acordo com alguns analistas *bitcoiners*, o Bitcoin pode estar oficialmente entrando no *"Slope Of Enlightenment" (figura anterior).* A "inclinação/tendência" é uma das etapas de um ciclo tecnológico descoberto pela empresa líder em pesquisa e consultoria Gartner, o *Gartner Hype Cycle*[395]:

Com esta ferramenta metodológica, executivos, investidores, *traders* e pesquisadores possuirão a capacidade de filtrar o ciclo de FUD/FOMO na adoção de tecnologias. Por isso que é a metodologia que ajuda a entender o processo de maturidade e adoção das inovações.

Uma compreensão adequada do ciclo de hype permite que os investidores reduzam e aumentem o risco e aumente lucratividade, operando do lado oposto das falhas emocionais. Essa mesma fonte, afirma que o Bitcoin pode ter já passado pelo "Vale da Desilusão" e agora estaria entrando na fase de "esclarecimento" (*Slope Of Enlightenment*).

3) Adoção, volatilidade e hiperbitcoinização

“Reclamar que bitcoin é volátil é como
reclamar que o céu é azul.”

Hiperbitcoinização é o momento em que o BTC não corrige mais em *fiat* e ninguém estará mais disposto a trocar BTC por qualquer quantidade de *fiat*, como aconteceu em bolívares.

Distribuição de conhecimento e ondas de adoção e infraestrutura são recíprocas, formando um *loop* de *feedback* virtuoso e uma função de tempo e valor. À medida que o valor aumenta, o Bitcoin capta o interesse e a atenção de um público muito mais amplo de potenciais adotantes, que então começam a aprender sobre os fundamentos do Bitcoin.

Da mesma forma, uma base de ativos valorizada atrai capital adicional não apenas como uma reserva de riqueza, mas também para construir uma infraestrutura incremental (por exemplo, desenvolvimento tecnológico, mercado de compra e venda *Exchanges*, soluções de custódia, camadas de pagamentos, *hardware*, mineração etc).

No momento, o Bitcoin ainda é incipiente e a base de usuários provavelmente represente em torno de 1% a 2% do potencial global (em um mundo com 7,8 bilhões de habitantes e 70% adultos). Quando um bilhão de pessoas adotarem o Bitcoin, a noção da grandeza do seu valor decorrente do Efeito Rede será conhecida. Até lá, ciclos de alta volatilidade tendem a ocorrer (mesmo que decrescentes em termos reais e não em *fiat*) com os agentes aprendendo a precificar o ativo em um mercado cada vez maior, mais líquido e mais desenvolvido.

A volatilidade[396] do bitcoin em termos reais só diminuirá à medida que atingir a maturidade e a taxa de adoção se estabilizar – a redução da volatilidade no poder de compra se dará ao longo do tempo. Ou seja, se um bilhão de pessoas usarem bitcoin, os 100 milhões de adotantes subsequentes representarão apenas 10% adicionais da base. Tendo em vista que o fornecimento de bitcoin permanece com um cronograma fixo da sua oferta monetária, Charles Vollum, da *Pricedin Gold*[397], vem notando o declínio da volatilidade sobre a existência do bitcoin, novamente com o preço tanto em dólar como em ouro**:**

> Em 2011, o limite superior era cerca de 84x o limite inferior. Um ano depois, a proporção era de 47x. Em 2015, era 22x, e no início de 2020 havia caído para 12x. Isso é bom, demonstrando um declínio na volatilidade geral de pico ao vale. Se esse padrão persistir, a proporção será de cerca de 9x em meados de 2024 e cerca de 6,5x até o final da década. Ainda alto pelos padrões de *forex* e títulos, mas menos de 10% da volatilidade de 2011!

Enquanto a volatilidade em *fiat* é inevitável, sendo uma característica de qualquer ativo novo com características singulares (e não um *bug*), o influenciador *bitcoiner* e ex-engenheiro do *Google*, Vijay Boyapati, explicou no *podcast* de Stephan Livera[398] que "Os economistas do *establishment* ridicularizam o fato de que o bitcoin é volátil, como se você pudesse ir de algo que não existia para uma forma estável de dinheiro da noite para o dia; é completamente ridículo".

O que acontece entre as ondas de adoção é a função natural da descoberta de preços, à medida que o mercado converge para um novo equilíbrio, que nunca é estático. Nos ciclos de *hype* do Bitcoin, a ascensão, a queda, a estabilização e novamente a subida são quase rítmicas. Também são naturalmente explicadas pelo medo especulativo, seguido pelo acúmulo de conhecimento fundamental e pela adição de infraestrutura incremental. Roma não foi construída em um dia; no bitcoin, a volatilidade e a descoberta de preços são fundamentais para o processo.

Enquanto o Bitcoin vai adquirindo uma parcela na competição global por reserva de valor por conta de suas propriedades monetárias superiores, a função de uma economia é acumular capital que realmente torne nossas vidas melhores, não dinheiro. O dinheiro é meramente o bem econômico que permite que a coordenação acumule esse capital. Como o bitcoin é uma forma de dinheiro fundamentalmente superior, ele tende a ganhar poder de compra em relação aos ativos monetários inferiores (e substitutos monetários) e a ganhar cada vez mais participação de mercado na função de coordenação econômica, apesar de ser menos funcional como moeda transacional hoje.

O Bitcoin tende a se tornar moeda transacional ao longo do tempo. Nesse período de transição, seria muito mais lógico gastar um ativo depreciável (dólares, euro, iene, real, por exemplo) e economizar um ativo de valorização (bitcoin), seguindo o princípio monetário da Lei de

Gresham[399], que diz: “A má moeda tende a expulsar do mercado a boa moeda”. Num contexto destes, a Lei de Gresham prevê a ocorrência de um fenômeno de conservação por parte dos agentes da moeda “boa”, enquanto a moeda “má” é utilizada para efetuar os pagamentos (a exemplo do fenômeno do bimetalismo, em que a prata tinha mais velocidade de circulação como moeda de pagamento que o ouro, que passou a servir como reserva de valor).

Na trajetória do Bitcoin para a monetização completa, a reserva de valor deve vir como uma primeira ordem lógica, e o Bitcoin provou ser uma boa reserva de valor, apesar de sua volatilidade. À medida que a adoção amadurecer, a volatilidade relativa naturalmente cairá e *satoshis* se tornarão cada vez mais meio de troca direta. Como afirma Taleb: “Sistemas complexos que suprimiram artificialmente a volatilidade tendem a se tornar extremamente frágeis, enquanto ao mesmo tempo não exibem riscos visíveis.”

Em política monetária, as funções básicas de moeda são: 1º: reserva de valor, 2º: meio de troca e 3º: unidade de conta.

Se há uma bolha que deveria te preocupar, não deveria ser a bolha do bitcoin. “Bitcoin não é bolha, é a agulha que vai estourar a bolha das bolhas – a bolha do juro negativo, a bolha do consumismo, a bolha imobiliária, a bolha das ações, a bolha da previdência, a bolha dos títulos, a bolha do *welfare*; e a bolha do endividamento”.

Se o ativo permanecer seguindo seu padrão histórico, deve continuar tendo períodos de valorização exponencial seguidos de correções violentas, como já houve de até 90% (embora sejam menores as quedas posteriores), seguidas de períodos de acumulação (preço em lateralização).

Também é razoável considerar que, quanto maior for o seu valor de mercado e o seu grau de legitimação – como aconteceu com os mercados futuros da CBOE/CME em 2017 e aconteceu em 2020 com o início da negociação dos *ETFs* (*exchange-traded funds)* –, maior será a tendência de redução de volatilidade média com o tempo. Nassim Taleb, em seu livro *Skin in the game*, diz que “Coisas voláteis não são necessariamente arriscadas, e o inverso também é verdade”.

Em um cenário de hiperbitcoinização, haverá cinco classes de indivíduos:

a) Os Hugo Stinnes: alavancados maciçamente, na medida que a gestão de risco permite, serão premiados com aumento absurdo do patrimônio, como já ocorre com Saylor;
b) Os HODLers: experimentarão aumento absurdo do patrimônio, mas com muito menos risco;
c) Os *boomers* do *cash-and-carry:* receberão um prêmio de consolação (ex: rendimento de 100% numa moeda que perdeu 90% do poder de compra na hiperbitcoinização, ou seja, mitigarão a perda de 90 para 80%);
d) Os “diluídos”: verão o patrimônio alocado em ativos denominados em moeda *fiat* ou equivalentes (CDBs, dívida monetária, fundos de pensão etc) virar pó;
e) A turma da “carona”: que tem patrimônio não denominado em moeda (donos de imóveis e outros bens não-financeiros). Poderão ter leve aumento ou queda do patrimônio a depender de qual destes fatores será mais forte: a perda do prêmio monetário atribuído ao bem (imóveis, FIIs e ações); ou o ganho de prosperidade generalizado.

4) A demanda institucional: fase 4

> As empresas precisam do Bitcoin para proteger seus balanços. Enquanto os governos competem para desvalorizar suas moedas, muitas empresas não conseguem gerar um retorno positivo sobre o capital. Bitcoin protege a tesouraria.
>
> Brandon Quittem

A "fase 4"[400] do bitcoin ficou muito clara entre 2020 e 2021, com forte demanda institucional. Além do exemplo do GBTC da *Grayscale*[401] (viabilizando até recursos de *401k* e *IRA* serem alocados em bitcoins), empresas como *Microstrategy* de Michael Saylor, que virou grande entusiasta do Bitcoin; *Square* dirigida por Jack Dorsey grande defensor do Bitcoin, e diretor executivo do *Twitter*; *Tesla* comandada pelo polêmico Elon Musk; e até o Mercado Livre, uma das maiores empresa da América latina, e demais empresas[402] e gestoras de investimento adicionaram bitcoins a seus balanços.

Como mencionado, até mesmo a *BlackRock* (maior gestora de ativos do mundo) e outras gigantes estão começando a se expor ao Bitcoin, como *Citigroup*, *Paypal*, *Visa*, *Goldman Sachs*, *Morgan Stanley*, *Fidelity* e *JP Morgan.* Eventualmente, quem não a adicionar bitcoin às carteiras de clientes não vai ter como competir, caso os retornos históricos se mantenham.

Após fundos de BTC como o GBTC, a próxima etapa é o lançamento de *ETFs* (*Exchange-Traded Fund*, também conhecidos como fundos de índice, negociado em bolsa) de BTC – com menores taxas de administração e maior segurança para investidor de varejo e institucional. Essa foi a causa do encerramento das captações e o deságio sistemático do GBTC da *Grayscale*.

Dentre os *ETFs* e fundos com alguma exposição ao Bitcoin, podem ser citadas as brasileiras[403]: *Hash Dex* sob o código *HASH11* (fundo composto por bitcoin mais uma cesta de *altcoins* que mudam constantemente) e o produto da Q*R Asset Management*, da gestora de recursos da holding *QR Capital* sob o código *QTBC11* (100% bitcoin).

O Canadá também aprovou seu primeiro ETF de bitcoin da América do Norte e o primeiro do mundo, o *Purpose Bitcoin ETF* sob o código *BTCC* (acessível a cidadãos americanos e demais investidores, inclusive brasileiros, credenciados em *brokers* nos EUA, sob o código *BTCC.U-TO*).

5) Como analisar o mercado de bitcoin: FOMO e FUD

O bitcoin provou ser um ativo cíclico, com altas consideráveis de preços em períodos de *Bull Market* (mercado de alta). Em todos os estágios desses ciclos, há grupos de pessoas comprando, vendendo, fazendo *hodl*, negociando e minerando bitcoin. Para compreender totalmente a psicologia e as características desses ciclos de mercado, existem conjuntos de dados mais adequados para analisar além próprio livro-razão (*blockchain*) do Bitcoin. É possível explorar algumas métricas *on-chain* selecionadas que fornecem uma visão sobre sentimentos e os padrões de *hodlers*, especuladores e mineradores em sites como: *Skew, Coinmetrics e Glassnode*.

Há um ponto relevante a ser observado numa análise de mercado: *early adopters e smart money*, possuem um *modus operandi* semelhante (comprando em fundo e desovando em topos, como é evidente por análises *onchain*). Os compradores recentes de varejo que tendem a vender com perdas, as sardinhas.

O bitcoin tem um ciclo de, aproximadamente, 4 anos. Em cada um desses ciclos ou Eras, o preço passa a maior parte do tempo caindo (*bear barket*) e lateralizando. Nos 12 a 18 meses após o *halvening* há subida (*bull market*). O choque na oferta dos novos bitcoins (oferta marginal cai à metade) é o gatilho para aumento de preço que, quando passa dos padrões fundamentais, reverte para correção – igualmente exacerbada por ciclos emocionais[404]:

WALL ST. CHEAT SHEET™ WE'VE GOT THE WORD ON THE STREET
PSYCHOLOGY OF A MARKET CYCLE
THE FEELINGS APPEARING AS THE MARKET FLUCTUATES.
SIMPLIFIED MARKET CYCLE
Peak
Point of maximum financial risk
Recovery
Prosperity
Trough
Point of maximum financial opportunity
Contraction
Expansion
PRICE
TIME
Euphoria
I am a genius! We're all going to be rich!
Complacency
We just need to cool off for the next rally.
Thrill
I will buy more on margin. Gotta tell everyone to buy!
Anxiety
Why am I getting margin calls? This dip is taking longer than expected.
Belief
Time to get fully invested.
Denial
My investments are with great companies. They will come back.
Optimism
This rally is real.
Panic
Shit! Everyone is selling. I need to get out!
Hope
A recovery is possible.
Capitulation
I'm getting 100% out of the markets. I can't afford to lose more.
Disbelief
This is a sucker's rally.
Disbelief
This rally will fail like the others.
Anger
Who shorted the market?? Why did the government allow this to happen??
Depression
My retirement money is lost. How can we pay for all this new stuff? I am an idiot.
PRICE
TIME
WALL ST. CHEAT SHEET™
www.wallstcheatsheet.com

Se em 20 anos o fluxo líquido de dólares (seja nominal ou real) no ecossistema se mantiver, o bitcoin deverá custará 16x mais, *ceteris paribus* (considerando demais variáveis constantes). Para ficar claro: 16x mais a partir de US$50 mil seriam US$800 mil — ou seja, o BTC valer o equivalente a todo ouro no mundo.

Caso as moedas *fiats* morram, há o potencial de a riqueza nelas (US$ 100 trilhões) ser engolida pelo BTC e pelo ouro.

Voltando ao *halving*, toda vez que há redução da oferta marginal à metade, um novo processo de descoberta de preços (*bull run*) se inicial. A subida tem razão fundamental, mas qualquer ativo que sobe mais de 1.000% em um ano atrai gente que "comprou porque está subindo", causando o processo de excesso psicológico que o mercado chama de *FOMO* (*Fear of missing out*), ou "medo de ficar de fora".

Por isso, a cada ciclo, ocorre um momento de euforia que a cotação do bitcoin passa das métricas de análise técnica (como *Mayer multiple*)[405] e de análise fundamentalista (como *S2FX* e *S2F*)[406]. Quando a correção chega, as perdas são brutais, porque quem comprou pelo motivo de ter subido também vende porque está caindo. Neste caso há também um excesso psicológico que se chama *FUD (Fear, uncertainty and doubt)*, ou "medo, incerteza e dúvida". Em resumo, o preço do Bitcoin é impulsionado por dois fatores principais, oferta e demanda: a) escassez exponencial, com uma curva de oferta assintótica tendente a zero; e, b) a adoção crescente, com o percentual de usuários de Bitcoin em 2020 sendo equivalente ao de usuários da internet em 1997.[407]

Há quem acredite que os ciclos de subida de dezenas de vezes seguidos de quedas de mais de 85% vão ser amenizados com o tempo: como os defensores da Hiperbitcoinização[408] (em decorrência da hiperinflação) e do "super ciclo"[409] (considerando que compradores institucionais seriam menos emocionais, amenizando subidas e quedas).

6) Quais os riscos do Bitcoin?

O Bitcoin compartilha dos mesmos riscos dos demais ativos financeiros: a) riscos legais: ser proibido, criminalizado, eventual prisão ou pena de morte para quem usar; b) risco operacional, parar de funcionar por *bug*, ataque bem-sucedido ou colapso societal (inverno atômico provocado por guerra atômica, meteoro, ou massa coronal destruir a rede elétrica ou Internet mundial); c) crédito: o bitcoin não tem, porque não é *IOU* (*I owe you* – É geralmente um documento informal que reconhece uma dívida), não é dívida como real, é ativo como ouro, mas as empresas do ecossistema têm esse risco, de ficar sem financiamento[410]; d) liquidez: não ter quem queira ou consiga comprar ou vender, sem *gateways* para tirar ou colocar moeda no sistema (por exemplo, consequência de congelamento de ativos em *exchanges* como Mike Maloney acha que vai acontecer no *reset* ou "Plano Collor Mundial"); e e) risco de mercado: preço cair em recessão mundial, como ocorreu em março de 2020 quando o bitcoin caiu mais de 50% em menos de uma semana.

A volatilidade do bitcoin, em grande medida, é reflexo da percepção de risco do ativo e da infância no seu desenvolvimento e no aprendizado em seus mecanismos de descoberta de preços. Alguns[411] argumentam que, em decorrência desses fatores, a tendência é que sua volatilidade seja reduzida; outros defendem que, no final das moedas fiduciárias, o valor do bitcoin subiria exponencialmente (como o valor de qualquer ativo onde há hiperinflação a ponto de a sociedade se desmonetizar, como na Alemanha de Weimar, Zimbábue ou Venezuela), cenário usualmente denominado como hiperbitcoinização.

7) O padrão Bitcoin: Por que o Bitcoin é o rei?

Efeito rede, Efeito Lindy e Proof of Brain

A maioria das criptomoedas são originadas do código base do Bitcoin, cujos protocolo e *software* são publicados abertamente; e, assim, qualquer desenvolvedor em todo o mundo pode acessar o código e modificá-lo ou copiá-lo, no todo ou em parte, fazendo sua própria versão modificada do *software* Bitcoin.

A rede Bitcoin compartilha um registro público na sua “cadeia de bloco” (*blockchain/timechain*), que armazena de forma imutável todas as transações, desde o seu lançamento em 2009, operando 24h por dia e 7 dias por semana.

O advento do Bitcoin é digno de total respeito, como grande conquista da ciência da computação na tecnologia – ao atingir escassez digital pela primeira vez na história. Em suma, o código do Bitcoin garante que apenas um número definido de novos bitcoins seja emitido, sem intervalos, a cada 10 minutos, em média, enquanto a experiência tiver sucesso e houver alguém rodando o *software*.

Como uma moeda pode ser distinguida da outra? E o mais importante, como um investidor pode saber qual será o valor em longo prazo de uma moeda?

A proposta real de valor do Bitcoin é resumida por Jimmy Song[412] (2019): “Quase todos os projetos de *altcoin*, *ICO* ou *hard forks* pregam que estão sendo inovadores de alguma maneira ao afirmarem superioridade ao Bitcoin em algum aspecto. Porém, esquecem que a maior inovação já aconteceu”. Por essa razão, maximalistas consideram essas modalidades (*ICOs* e *altcoins*) como espécies de fraude e estelionato.

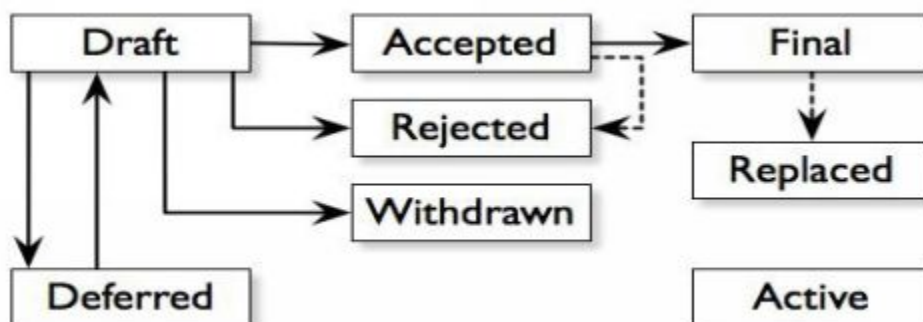
O Efeito Rede e o Efeito Lindy do Bitcoin são incomparáveis aos de outras criptomoedas, pois sua base de usuários (e por consequência maior capitalização de mercado), o número de *full nodes*, a capacidade de atrair melhores mentes em seu desenvolvimento *(Proof of Brain)*, seu ecossistema de negócios pujante com um mercado altamente inovador são muito maiores em qualquer métrica. Além disso, qualquer inovação ou melhoria das *altcoins* pode ser adotada no Bitcoin, como já aconteceu com a resolução do problema da maleabilidade e os *atomic swaps* entre *Litecoin* e *Decred*, por exemplo, que serviram de *testnets* para o Bitcoin com sucesso, mas desde então só tiveram seus valores em bitcoin em baixa para anos e anos. Como resume Vijay Boyapati[413]**:**

> Se o Bitcoin existir por 20 anos, haverá uma confiança quase universal de que estará disponível para sempre, da mesma forma que as pessoas acreditam que a Internet é uma característica permanente do mundo moderno.

A rede Bitcoin já possui um robusto *roadmap* de inovações – e muitas delas tendem a ser testadas antes em *altcoins* (além de sua *testnet*), demonstrando seus níveis de segurança e conservadorismo superiores.

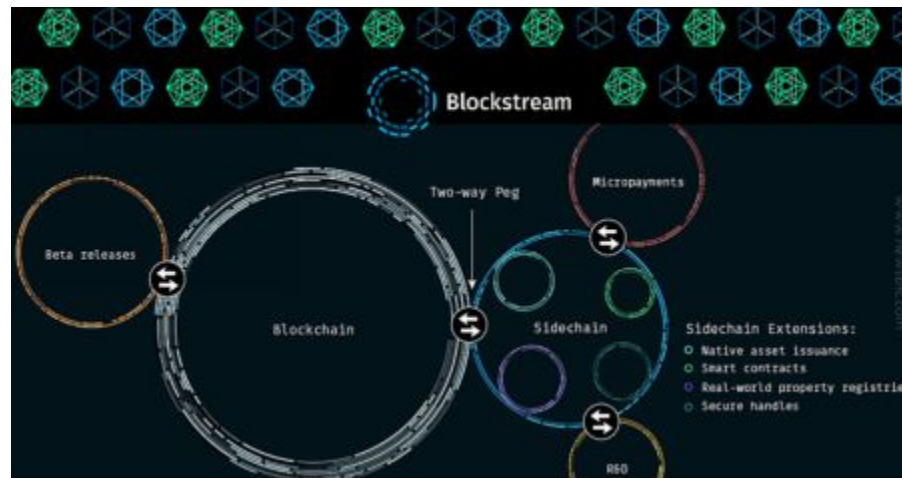
8) Roadmap e perspectivas: como escalar

Vários roteiros de desenvolvimento de inovações no Bitcoin já foram feitos desde 2015[414]. Essas metas não se cumprem integralmente – seja porque novas soluções superiores surgem ou por não haver implementação ou sequer desenvolvimento de propostas –, como se observa em diversas fontes jornalísticas, fóruns e relatórios financeiros[415].

BIP (Bitcoin Improvement Proposal) é uma maneira formal de transmitir sua ideia à comunidade de desenvolvimento. Os *BIPs* possuem um formato e modelos específicos e existe um editor *BIP* dedicado. Só porque um *BIP* é enviado não significa que ele será aprovado. Normalmente, este é o ciclo de vida do *BIP*[416]:

A autoria e o estado (rascunho, proposto, aceito, rejeitado…) de todos os BIPs (até agora do 1 ao 370) podem ser consultados publicamente[417], a maioria deles são incrementais e passam desapercebidos pelo usuário comum. Poucos são aqueles que mudam radicalmente tipos de endereços usados, funcionalidades ou custo de transação - como *SegWit* (BIP 141) e *Taproot* (BIP 343).

Os grandes focos dos BIPs recentes são: a) aumento de funcionalidades em *smart contract*s (facilitando *multsig*, *timelock* e soluções em outras camadas); b) redução de custo de transação e de tamanho das transações (aumento de eficiência); e, c) o aumento da fungibilidade, “monerização” do bitcoin.

Os grandes beneficiários desses BIPs são os projetos *Sidechain* (cadeias laterais) já operacionais, como as redes *RSK* e *Liquid***.** As cadeias laterais foram projetadas para permitir que outras *blockchains* se conectem à rede Bitcoin usando uma moeda separada que é referenciada ao bitcoin. Isto significa que cada *sidechain* é uma *blockchain* separada que pode ter regras diferentes da rede principal do Bitcoin enquanto ainda estiver conectada a ela. Isso permite que os usuários testem e desfrutem de novas funcionalidades de uma forma que não afete a *blockchain* principal, sem a necessidade de criar uma moeda digital.

Como ilustrado [418], são *sidechains* operacionais:

Liquid Network:[419] É uma *sidechain* privada, portanto, há algum controle sobre quem pode acessá-la. Os benefícios da *Liquid* são a permissão de transações instantâneas, a privacidade (transações confidenciais são incorporadas) e a capacidade de os usuários manterem fundos líquidos fora de uma *exchang*. Seu *token* é chamado de **LBTC** (*Liquid bitcoin*), sendo vinculado ao BTC na proporção de 1:1.

A rede se baseia no conceito "Cadeia Federada", que possui três partes principais no sistema: usuários; signatários de bloco, que são semelhantes aos mineradores; e vigias, que permitem que os fundos sejam transferidos para a cadeia de forma segura por meio de um processo conhecido como *pegging*. Foi desenvolvida pela empresa *Blockstream*.

***RSK (*Rootstock):**[420] É uma *sidechain* que planeja trazer funcionalidade de contrato inteligente e pagamentos quase instantâneos para a rede Bitcoin. Assim como a *Liquid*, ela usa um sistema federado, com os custodiantes rastreando o movimento do bitcoin entre a rede da *RSK* e a *mainnet* do Bitcoin. Ela faz isso usando um *token* chamado RBTC (Rootstock Bitcoin), que também é vinculado ao BTC na proporção de 1:1. Curiosamente, os contratos inteligentes no *RSK* são programados no *Solidity*, e a máquina virtual RSK é totalmente compatível com a da Ethereum. A rede da RSK é protegida por uma prova de trabalho, com o mesmo algoritmo do Bitcoin. Isso significa que as mineradoras de Bitcoin também podem dar segurança à rede *RSK* com muito pouco impacto no desempenho da mineração. A *RSK*

afirma ser capaz de escalonar para 100 transações por segundo usando verificação probabilística e provas de fraude, bem como *sharding*, algo que a Ethereum também está desenvolvendo. Anteriormente conhecida como *Rootstock*, a *RSK* é apoiada pela federação *RSK*, que é formada por mais de 30 empresas de *blockchain*, como *Xapo*, *Antpool*, *Bitpay e Digital Currency Group*. O CEO da *RSK* é Diego Gutierrez Zaldivar e foi lançada na rede Bitcoin em janeiro de 2018.

Dentre as melhorias recentes no Bitcoin, incluem-se:

***Segwit (Segregated Witness)*: Já implementado no protocolo do Bitcoin (via *soft fork*).** Foi proposta para além de mitigar um problema de limitação de tamanho de bloco na *blockchain*, que reduz a velocidade de transação do bitcoin (com isso demorando as confirmações na rede). O recurso também resolve o problema de maleabilidade das transações, dando espaço para a implementação de outras tecnologias de segunda camada, como a *Lightning Network*. Graças ao *SegWi*t e *batching*, as principais *exchanges* e *wallets* reduziram as taxas de transações na rede.

***Lightning Network*: Já possui aplicação prática[421].** Uma das propostas de solução em segunda camada para a rede do Bitcoin para dar escalabilidade, prometendo suportar um número quase ilimitado de transações fora da cadeia entre os usuários, e praticamente sem custos enquanto aproveita a segurança oferecida pela *Blockchain* do Bitcoin. Com “o futuro dos micropagamentos”, os usuários poderão comprar o tão “sonhado cafezinho na padaria” pagando frações ou quase nenhuma taxa de transação. Empresas como *Lightning Labs*, *Blockstream*, ACINQ e ZAP *Lighting* desenvolvem aplicações para a rede LN[422]:

Innovations in Bitcoin
Layer 2
Sidechains
Performance & Usability
Mining
Smart Contracts
Privacy
Channel Factories
eltoo
Atomic Swaps
Private Messages
Omni DEX
Microsoft ION
Open Timestamps
VeriBlock
Issued Assets
Lightning Network
Omni
Identity
Data Anchors
Rootstock
Drivechain
Elements
Liquid
MuSig
Cross-Input Aggregation
Schnorr Signatures
Neutrino
Erlay
BTCPay
uTreeXo, libMiniSketch, Tx Accumulators
FIBRE
BetterHash
Stratum
Mining Derivatives
Stratum V2
CheckTemplateVerify
tBTC
MAST/ Taproot
Scriptless Scripts
Simplicity
Ivy
Hivemind
CoinJoin
Dandelion
Confidential Transactions
CoinSwap
G'root
Tapscript
ZeroLink
P2EP
SNICKER
Value Shuffle
Bulletproofs
TumbleBit

> Bitcoin é o projeto mais ambicioso que a humanidade está construindo hoje - garantir os direitos de propriedade e o futuro financeiro de 7,8 bilhões de pessoas com nada além de um simples smartphone. @DocumentingBTC[423]

***Schnorr Signatures/Taproot*:** Agregam várias assinaturas de transações em uma única assinatura. Isso reduz um pouco o tamanho da transação (redução no tempo de confirmação das transações) e inibe chances de futuros ataques de *spam* na rede Bitcoin.

> A assinatura Schnorr é considerada o mais simples esquema de assinatura digital para ser comprovadamente segura em um modelo *de oráculo* aleatório. [2] É eficiente e gera assinaturas curtas. Ela foi coberta pela patente US 4.995.082, que expirou em fevereiro de 2008. Wikipédia**[424]**

As assinaturas de Schnorr trazem uma enorme melhoria em fungibilidade, privacidade, escalabilidade e funcionalidade. Finalmente, a implementação de assinaturas de *Schnorr* poderia permitir desenvolvimentos futuros para o Bitcoin, como contratos inteligentes.

O *Taproot*[425] permite pagamentos ao *hash* da chave pública, que pode opcionalmente ser passada para um *script*.

Moedas protegidas pela *Taproot* podem ser emitidas, seja cumprindo o *script*, seja fornecendo uma assinatura que é verificada contra a chave pública. O *Taproot* destina-se a ser utilizado com assinaturas Schnorr, o que simplifica a criação de *scripts* multipartidários (por exemplo, com *MultiSig*). O *soft fork* também deve permitir que a *Lightning Network* mude de HTLCs para *Payment Points*, o que também é uma grande melhoria para a *Lightning Network* em termos de privacidade.

Das implementações futuras, podem ser enumeradas:

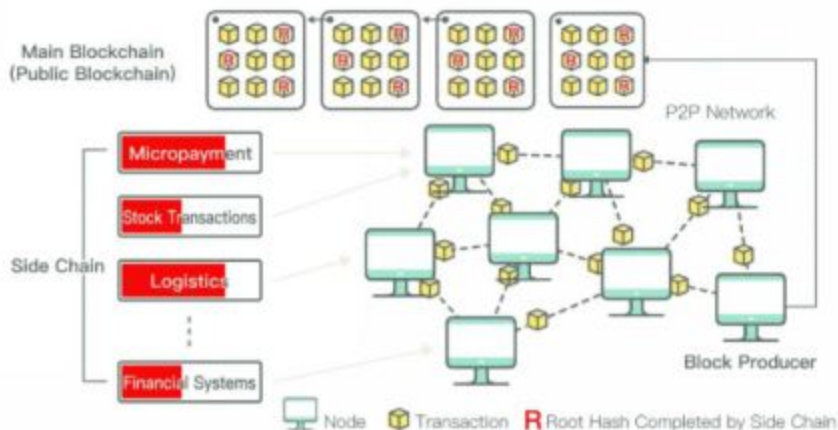
***Bulletproofs*: Ainda sem data definida, estando na fase de discussão e pesquisa entre desenvolvedores**. A tecnologia oculta quantidades de transações entre o remetente e o receptor para maior privacidade com o mínimo de poder computacional necessário para processar uma transação. Desenvolvido por Jonathan Bootle, da University College of London, e Benedikt Bünz, de Stanford, o *bulletproofs* é prova de conhecimento zero, o que significa que não se exige qualquer confiança entre as partes.

O *Bulletproofs* atraiu a atenção de outras criptomoedas, como Monero, que já implementou em seu protocolo, e Litecoin, que considera implementar. A tecnologia também é leve e não aumenta maciçamente a quantidade de energia computacional necessária para processar transações, podendo funcionar bem em *blockchain*s públicos como o Bitcoin.

***Confidential transactions* (CT): Ainda sem data definida, está na fase de discussão e pesquisa entre desenvolvedores**. As transações confidenciais (*TC*) manteriam as quantias de transações de bitcoins visíveis apenas entre os participantes da operação. A *CT* foi discutida por Adam Back, cofundador e *CEO* da *Blockstream*, em um fórum de discussão em 2013, sendo esse trabalho realizado pelo desenvolvedor Greg Maxwell. Em novembro de 2017, Maxwell anunciou que reduziu de 16 vezes o tamanho das transações (*CT*) normais de Bitcoin para apenas três vezes.

Drivechain: Ainda sem data definida, estando na fase de discussão e pesquisa entre desenvolvedores. O *Drivechain* planeja permitir que várias *blockchains* sejam vinculadas à *mainnet* do Bitcoin. Assim como a *RSK*, as cadeias laterais de *Drivechain* construídas podem ser protegidas por mineradores de Bitcoin usando mineração mesclada. Ao contrário da *RSK*, a

Drivechain é flexível e os desenvolvedores podem criar cadeias laterais *(sidechains)* adaptadas às especificações desejadas, como tamanhos de bloco maiores ou recursos de privacidade.

Essa implementação exigiria uma atualização no nível do protocolo, ou *soft fork*, e separa as alterações necessárias em duas partes: depósito de *hashrate* e mineração cega fundida. O *Drivechain* foi inventado por Paul Sztorc (que também criou o *Hivemind*), com a ajuda de Chris Stewart, Jason Dreyzehner, do *BitPay* e do desenvolvedor pseudônimo *Cryptaxe*.

***MAST*: Incorporada na atualização do pacote Taproot**.[426] *MAST é a* abreviação de *Merkelized Abstract Syntax Trees*, propõe melhorar o Bitcoin alterando a forma como os contratos inteligentes são gravados na *blockchain*. Com efeito, permite que os contratos inteligentes sejam divididos em suas partes individuais.

O *MAST* aumenta a privacidade mantendo partes ocultas e não utilizadas de contratos inteligentes, vinculando menos informações às chaves públicas. Também pode reduzir o tamanho da transação, uma vez que somente as partes preenchidas de um contrato inteligente são gravadas na *blockchain*. Finalmente, tem o benefício de permitir contratos inteligentes maiores. Bitcoin tem limites de tamanho de *byte* em *scripts*, o que limita seu tamanho geral. Mas, se um contrato inteligente pode ser quebrado em pedaços e escrito na *blockchain* em várias transações, então ele pode ser maior.

***Mimblewimble*: Ainda sem data definida, estando na fase de discussão e pesquisa entre desenvolvedores**. Oferece privacidade por padrão, mais fungibilidade[427] e melhor capacidade de escala da rede.

Como não oferece suporte a *scripts*, ele provavelmente seria implementado como uma *sidechain*.

8.1) Camada base (*onchain*), 2º camada e *sidechain* (cadeia laterais):

Numa rede monetária, é inevitável o "Trilema da Escalabilidade"[428]: segurança, descentralização e velocidade.

É impossível maximizar todos os três ao mesmo tempo numa só camada. Por *design*, foram priorizadas a segurança e a descentralização na camada base do Bitcoin.

Para viabilizar os três atributos, a rede precisa que outros protocolos sejam construídos em cima do protocolo base principal (seguro e descentralizado). Assim, os três atributos podem ser alcançados por meio de camadas superiores (2ª camada e *sidechains*), na qual cada uma irá priorizar atributos específicos. Como Hal Finney já expressava desde 2010.[429]

Como Nick Szabo[430] já expressava em 2017, registros *onchain* são a camada mais segura, como o *swift* para o sistema bancário, que possibilita as demais transações menos criticas serem liquidadas internamente. A camada base (*layer* 1) precisa ser a mais sólida e segura possível, sua falha seria a morte do sistema. Para a camada 2 e *sidechains*, pode haver menos segurança e mais velocidade e flexibilidade.

Operar *onchain* em alguns anos vai ser tão comum quanto transferir bens em cartório ou fazer remessas via *Swift*. *Sidechains* e 2ª camada, como a rede *liquid network* e *lightning network*, permitem transações ilimitadas em fração de segundo por centavos ou grátis, são seguras e permitem a privacidade nas transações.

O Bitcoin é a camada base para tokens mais eficientes em seus respectivos nichos: a) há mais de 2.300 BTCs aportados (Capacidade de rede)[431] na *Lighting Network*, que consomem milhões de vezes menos transações do que uma operação de cartão de crédito; b) há mais de 3.200 LBTC na *Liquid Network*, com *fee* fixa (equivalente a 1 satoshi/vbyte), blocos a cada 1 minuto e *confidential transacionas;* e, há mais de 2.020 RBTC na *RSK*[432].

Outros exemplos de protocolos construídos em cima da rede principal do Bitcoin, soluções de 2ª camada e *sidechains*, sejam elas já construídas ou em andamento são: a) *drivechains*[433]; b) *statechains* [434]; e, c) contratos inteligentes RGB[435]; d) Impervious[436]; e) *Stacks*[437].

Produtos já operantes em 2ª camada / *Sidechains* / *Discreet log contracts (DLCs)*:

- *SovrynBTC*
- *RSKsmart*
- *RIF Network*
- *Rsk Swap*
- *Moneyonchaino*
- *Wallets lightning network*
- Plataforma de Derivativos LNM e Kollider
- *Wallet RGB* (em construção)
- *Atomic Finance*
- *Suredbits*
- Dentre outros...

9) Stock to Flow (S2F) & S2FX – bitcoin valuations

“Todos os modelos são falhos, mas alguns são úteis."
George Box

O modelo *Stock-to-Flow* do Bitcoin foi construído pelo misterioso investidor institucional cuja personalidade no *Twitter* é conhecida apenas como *PlanB*[438], com artigos publicados em seu *blog* no *Medium*[439] (/*@100trillionUSD*), onde o leitor pode pesquisar e entender mais sobre a proposta de modelo para precificar o Bitcoin.

Este modelo trata o Bitcoin como comparável a *commodities* como ouro, prata ou platina. São conhecidas como mercadorias de “reserva de valor”, porque retêm valor por longos períodos devido à sua relativa escassez.

O *Stock to Flow (S2F)* mostra quantos anos são necessários para a taxa de produção atual atingir o estoque (reservas existentes), portanto, uma relação consistente entre razão de estoque e fluxo e o respectivo preço (medido pelo *market cap* total do ativo).

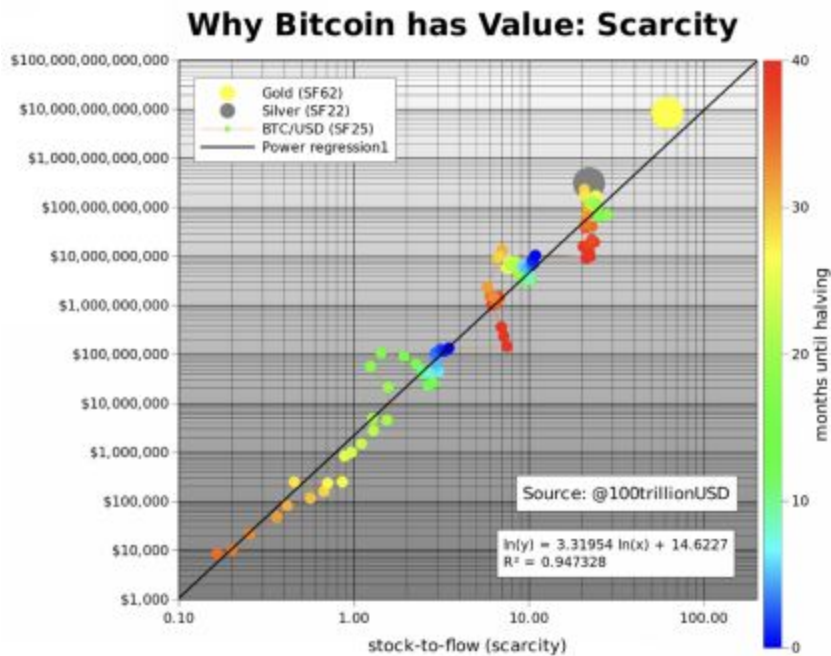
Aplicando ao bitcoin, como sua razão de escassez é crescente e predeterminada, métodos de avaliação com valores exponencialmente maiores foram desenvolvidos, aplicando as correlações identificadas em outros ativos.

A definição de escassez no dicionário remete a de algo difícil de ser encontrado na natureza ou reproduzido em laboratório; muito similar aos metais preciosos. Quando algo se torna escasso o suficiente, pode ser usado como dinheiro. A relação entre estoque e fluxo (*S2F*) é definida como a divisão entre a produção anual e o estoque atual.

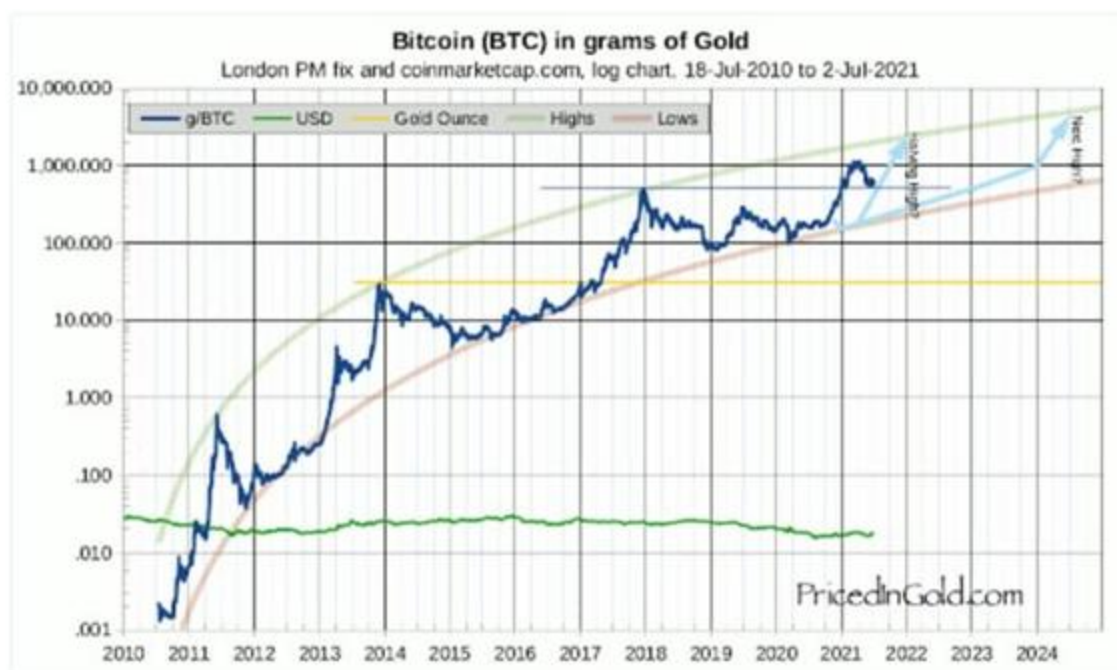
_SF_ = estoque / fluxo

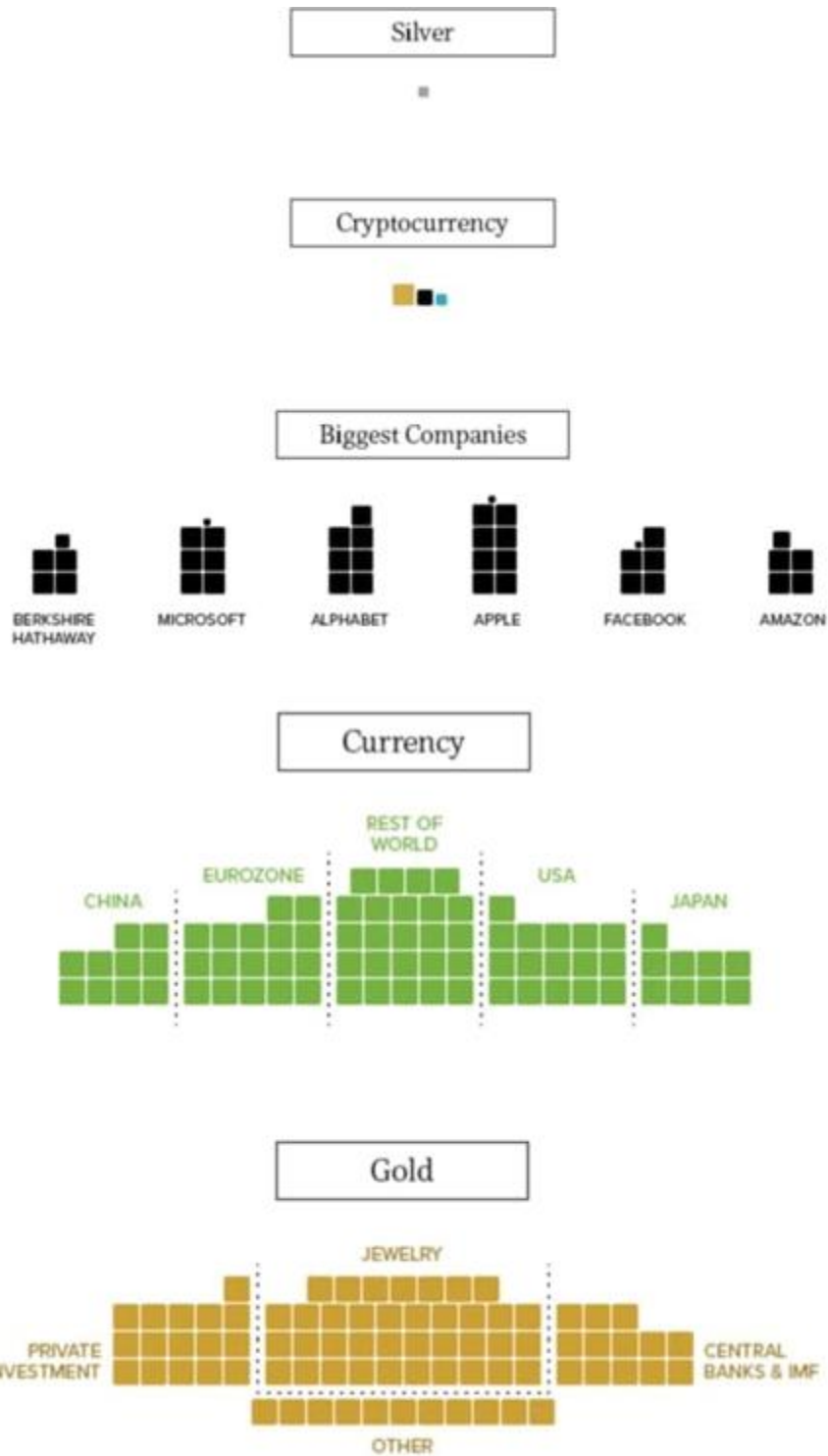
O uso do modelo bitcoin *S2F* não é realmente para negociação, mas para operações táticas de alocação de ativos.

Após a demonstração formal de que o modelo do *S2F* não tinha valor preditivo[440] e que, dentre outros problemas, o *S2F* deriva do preço e não o oposto (relação de correlação e não causalidade), o autor tentou contornar o problema com o *S2FX – Stock to Flow Cross Asset Model* (usando relações

entre ativos, sem variável de tempo).

Existem dezenas de modelos preditivos como o *FF*, *bitcoin rainbow chart*, *Bitcoin VWAP price*, *CVDD* e outros[441] – usualmente apresentando padrões exponenciais.

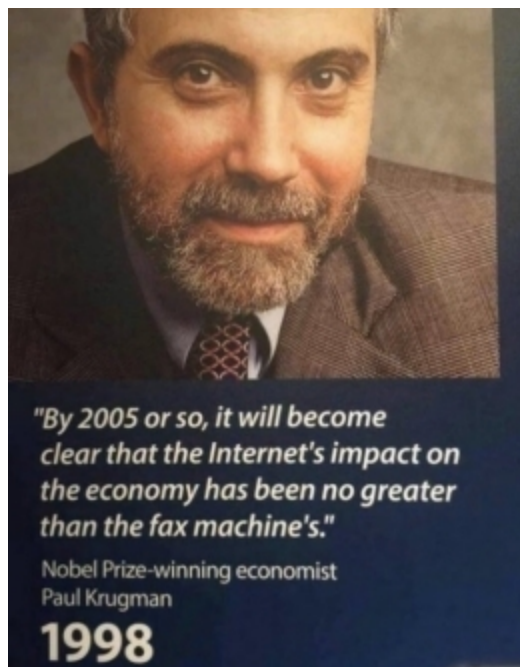
Outro modelo com grandes evidências lógicas e empíricas é o *valuation* pelo custo mínimo de mineração[442]. O racional é que mineradores[443], em regra, não operariam no prejuízo e o valor mínimo de mineração seria um valor “piso" para a cotação do bitcoin – embora a autocorrelação entre preço e cotação possa tornar essa causalidade espúria[444]:

Charles Vollum, da *PricedindGold.com*, sugere em um artigo[445] um aumento de mais de 10x nos próximos anos (se voltar ao topo da faixa histórica), o que implicaria um preço em dólar de seis dígitos (como o modelo do *PlanB*), se o ouro permanecer relativamente estático em termos de dólar. No entanto, ele também observa que historicamente tem sido menos explosivo em cada ciclo (em gramas de ouro):

> Minha análise começa observando as alturas e os tempos relativos das elevações em meados de 2011, final de 2013 e final de 2017. O segundo pico é cerca de 48 vezes maior que o primeiro, enquanto o terceiro pico é de cerca de 17x o segundo. Portanto, a taxa de crescimento nos picos parece estar diminuindo.
>
> Chales Vollum

Irrelevância do Bitcoin nos mercados[446]

10) Ameaças ao Bitcoin

Existe um rol de centenas de pessoas que já decretaram a morte do bitcoin, desde ganhadores de prêmio Nobel, *CEOs* de grandes corporações e

líderes políticos mundiais. Todos erraram e, até agora, viraram alvo de risos e piadas. A lista de obituários do bitcoin (*bitcoin-obituaries*)[447] conta com inúmeros registros de "decretação" da morte do Bitcoin em mídias de grande circulação.

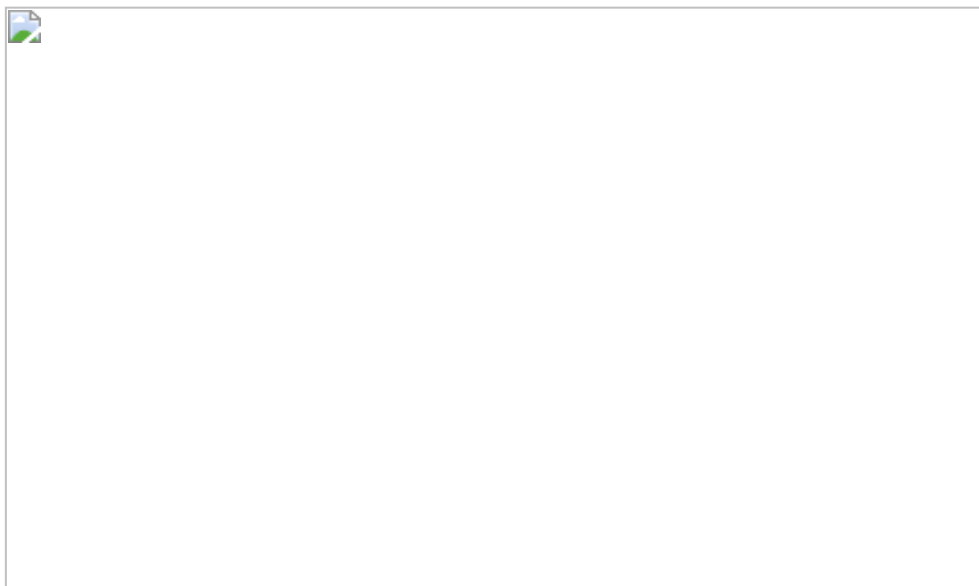
O destaque nessa categoria de "vergonha alheia", ou como prefere Taleb "*intelectual yet idiot*", é Paul Krugman – que, em 1998, também disse que a Internet não iria mudar a economia mais do que o aparelho de fax.

O Bitcoin pode ser destruído caso a rede mundial de computadores seja comprometida, assim como também será comprometido o resto da economia mundial.

Se a criptografia do Bitcoin for comprometida por computação quântica[448], as dos governos e bancos também serão (e com valores bem mais significativos).

Se o fornecimento global de energia elétrica for comprometido, a última preocupação de um ser humano será o Bitcoin – já que voltaríamos em semanas aos níveis tecnológicos e à capacidade de suporte do século XVII, com a maioria das pessoas no mundo mortas de fome ou em decorrência do caos.

Como todo ativo financeiro, o bitcoin está exposto a riscos operacionais (como *bugs*), legais (ser criminalizado) e de mercado (fortes variações de cotação). Como o bitcoin é um *token* de uso – e não de *equity* nem de dívida –, não carrega risco de liquidez nem de crédito, embora contratos (como empréstimos colateralizados) e empresas do ecossistema apresentem esses riscos, visto que nesses casos as chaves-privadas estão na posse de terceiros.

Se o Bitcoin não tivesse riscos inerentes, não teria o potencial de ganho sistemático já comprovado. O bitcoin é um *hedge*, um seguro, contra o sistema convencional por não apresentar correlação relevante com os ativos tradicionais e tender a performar melhor quanto piores forem as decisões de governos. Também por isso já se defende que é uma nova categoria de ativo.

A taxa de adoção de novas tecnologias usualmente segue curva em U invertido: primeiro com adoção exponencial de criadores pioneiros, *early adopters*, *smart money*; e, só por fim, da maioria das pessoas, como ilustrado na *Roger's Bell Curve*[449]:

As figuras anteriores demonstram como em 2020 o valor de mercado do Bitcoin ainda é irrelevante, se comparado a outros mercados e até a algumas empresas. Não há como prever se sua evolução exponencial vai encontrar um platô em termos reais (curva S da maioria das tecnologias) ou se vai continuar aumentando em termos nominais em *fiat*, como previsto na hiperbitcoinização (curva em J).

Não há como prever se o Bitcoin vai morrer ou se será o início da conversão de praticamente todos os ativos para as nuvens. O que se pode afirmar com certeza é que o Bitcoin resolveu demandas que existiam desde o milênio passado (dinheiro digital descentralizado de Friedman e moeda privada imune à jurisdição de Hayek) com a solução do problema de confiança mútua dos generais bizantinos, e sua tecnologia não será facilmente esquecida. Agora a humanidade não vai depender mais da confiança de terceiros para ter acesso à reserva de valor transmissível por qualquer meio de comunicação, mantida e autenticada sem qualquer custo de corretagem ou administração.

Bem-vindo à Era Digital, parabéns por descobrir o Bitcoin antes da maioria das pessoas. Nos próximos anos, ficará claro quem vai ganhar a corrida tecnológica: se os governos e grandes corporações, cada vez mais totalitários e corruptos, ou os indivíduos. Só depende das nossas decisões no presente – se uma qualidade suficiente de produtores se recusar a financiar os parasitas, ficará claro que Satoshi Nakamoto é John Galt, provocando o colapso dos Estados Sociais.

Ou o Bitcoin tirará dos governos o poder de criar moeda, de se endividar e de controlar taxas de juros, propiciando um renascimento moral, tecnológico e material, com mudanças brutais das preferências temporais derivadas do acesso a boas reservas de valor; ou a humanidade experimentará decadência moral, tecnológica e material, em um período de totalitarismo sem precedentes, com governos recebendo informações de grandes corporações e usando gamificação para motivar competição agressiva de obediência e eliminação de dissidentes.

Você pode levar um ser humano à autossoberania, mas não pode fazê-lo suportar o ônus da responsabilidade pessoal.
Jameson Lopp

Se você não acredita em mim ou não entende, eu não tenho tempo para tentar te convencer, desculpe-me… (HFSP)
Satoshi Nakamoto

DICAS COMPLEMENTARES

Livros:

- *The Bitcoin Standard* (Saifedean Ammous)
- *The Fiat Standard* (Saifedean Ammous)
- Bitcoin – A moeda na era digital (Fernando Ulrich)
- *The Ethics of Money Production (Jörg Guido Hülsmann)*
- *The Price of Tomorrow: Why Deflation is the Key to an Abundant Future* (Jeff Booth)
- O que o Governo Fez com o Nosso Dinheiro (Murray Rothbard)
- *Mastering Bitcoin (*Andreas Antonopoulos*)*
- *Grokking Bitcoin (Kalle Rosenbaum)*
- Bitcoin - A Internet do Dinheiro (*Andreas Antonopoulos)*
- *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money (Nathaniel Popper)*
- *Bitcoin Billionaires: A True Story of Genius, Betrayal and Redemption (Ben Mezrich)*
- *Bitcoin Money: A Tale of Bitville Discovering Good Money (Michael Caras)*
- *From Bitcoin to Burning Man and Beyond (John H. Clippinger)*
- *Trilema*: www.trilema.com/category/bitcoin/ *(*Mircea Popescu*)*
- *The Little Bitcoin Book* (Luis Buenaventura e Jimmy Song*)*
- *Thank God for Bitcoin (*Jimmy Song, Gabe Higgins e outros*)*
- *The Blocksize War (*Jonathan Bier*)*
- *The Bullish Case for Bitcoin (*Vijay Boyapati*)*
- *Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies (*Nik Bhatia*)*

Filmes e Séries:

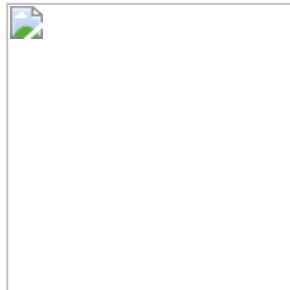
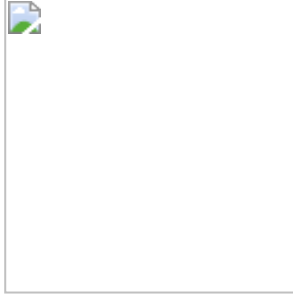
- Bitcoin: O Fim do Dinheiro como Conhecemos (*Bitchute*)
- *The Bitcoin Gospel (YouTube)*
- *Hidden Secrets of Money (YouTube)*
- *Banking on Bitcoin (Netflix)*
- *The Rise and Rise of Bitcoin (Vimeo)*
- *Ulterior States (YouTube)*
- *The Internet´s own Boy (HBO)*
- *TPB AFK (YouTube)*
- *Hard Money Film (Vimeo)*

POSFÁCIO

Se gostou do conteúdo, envie um *e-mail* (bitcoinblackpill@protonmail.com) ou ingresse no grupo do *Telegram* (Bitcoinblackpill_BR) para receber as publicações subsequentes.

Para referências completas e imagens coloridas e com alta definição,
Acesse nosso site: www.bitcoinblackpill.com

Gostaria de reconhecer o nosso trabalho de alguma forma?

Financie continuidade do projeto:

Doe Bitcoin pela Lightning Network

Endereço bitcoin:
bc1qptfh5hrnyasty7l2c3xta5cpvsrralm98z7243

ANEXOS

ANEXO I: Cartilha do MPF sobre criptos: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/cartilhas/atuacao-interinstitucional-com-o-bb/cartilha-moeda-digital-versaoatual.pdf.

ANEXO II: Criptomoedas, orientações gerais para equipes de buscas (Polícia Federal do Brasil): https://www.criptofacil.com/wp-content/uploads/2019/04/1_5046474950894944324-2.pdf.

ANEXO III: *3 Reasons I'm Investing in Bitcoin*: https://www.lynalden.com/invest-in-bitcoin/ - (arquivado: https://archive.vn/TXeuS).

ANEXO IV: Paul Tudor Jones: *The Most Compelling Case For Owning Bitcoin:* https://seekingalpha.com/article/4345426-paul-tudor-jones-compelling-case-for-owning-bitcoin - (arquivado: https://archive.vn/EcKsL).

ANEXO V: Parker Lewis: *Gradually, then Suddenly:* https://drive.google.com/file/d/1hcWezZLPV5MUQ_btezCv6p_H5g9loSUF/view - (arquivado: https://archive.vn/EMq8n).

ANEXO VI: *Bitcoin Investment Cases of Fidelity, Grayscale, VanEck, MicroStrategy:* https://github.com/100trillionUSD/bitcoin/find/master.

APÊNDICE: Resumo Tributário

Não é possível regular ou controlar diretamente o uso privado dos criptoativos, pois os *tokens* podem ser transferidos para qualquer país em minutos via Internet, por telefone, satélite, rádio ou até por memorização da *seed phrase*. A regulação estatal atua sobre as instituições formais submetidas à soberania estatal – corretoras, *gateways*, *P2P*, serviços de custódia ou contribuintes, pessoas naturais, que prestem voluntariamente as suas informações.

Abaixo seguem as normas regulatórias da Receita Federal:

Tributos - pagamentos - SRF/IN 84 de 2001

IR – ganhos de capital em outros direitos:
Isento até R$ 35.000 por mês;
de 35 mil até 5 Milhões, 15%;
de 5 a 10MM, 17.5%;
de 10 a 30MM, 20%;
Acima de 30MM, 22,5%

Procedimento atual: declara pelo GCAP, gera DARF e paga até o mês posterior.

INSTRUÇÃO NORMATIVA Nº 1.888 DE 2019
Tributos - compliance – Receita Federal do Brasil

GLOSSÁRIO

1. Altcoin: Criptomoeda alternativa, criada após o Bitcoin.

2. Ataque de 51%: Um ataque de 51% pode ser executado contra rede blockchain que utiliza o algoritmo de consenso PoW, no qual uma única entidade ou organização consegue controlar a maioria do hashrate, podendo causar e explorar falhas no sistema. O atacante teria os seguintes poderes: poder de mineração suficiente para excluir ou modificar a ordem das transações de forma intencional; fazer retroceder transações, o que poderia acarretar um problema de double-spending (gasto duplo); o fraudador pode impedir que algumas ou todas as transações sejam confirmadas (processo conhecido como ataque de negação de serviço) ou impedir que alguns ou todos os mineradores continuem seu trabalho, monopolizando mineração. O atacante não pode: reverter transações de outros usuários ou impedir que novas transações sejam criadas e transmitidas à rede; criar moedas do nada; mudar a recompensa dos blocos; ou roubar moedas que nunca lhe pertenceram.

3. AT (Análise técnica): Análise Técnica é uma ferramenta utilizada tanto por especuladores profissionais, como por amadores para análise do movimento de preço de alguns ativos financeiros, com base na oferta e procura destes.

4. *AML* (*Anti Money Laundering* – Antilavagem de Dinheiro): É um termo que se refere às regulamentações impostas em uma indústria financeira, em um esforço para prevenir e deter atividades ilegais. A lavagem de dinheiro indica ocultar a origem dos fundos. Diferentes jurisdições usam diferentes leis de *AML* para garantir que dinheiro “sujo” não seja recolocado no sistema.

5. Alavancagem (*leverage*): É uma estratégia de investimento que usa dinheiro emprestado – especificamente, o uso de vários instrumentos financeiros ou capital emprestado – para aumentar o potencial retorno de um investimento.

6. Algoritmos: Um algoritmo é uma sequência finita de ações executáveis que visam obter uma solução para um determinado tipo de problema.

7. Arbitragem (*arbitrage*): É a compra e venda de um ativo para lucrar com uma diferença no preço entre mercados. É uma operação que lucra

explorando as diferenças de preço de instrumentos financeiros idênticos ou similares em diferentes mercados ou de diferentes formas. A arbitragem existe como resultado de ineficiências do mercado e, portanto, não existiria se todos os mercados fossem perfeitamente eficientes.

8. Antifrágeis: Coisas que se beneficiam com o caos. A antifragilidade, um neologismo proposto por Taleb, seria o exato oposto da fragilidade, estando além da resiliência ou da robustez. O resiliente resiste a choques e ao tempo e permanece o mesmo, o antifrágil fica melhor. Esta propriedade estaria por trás de muitas coisas que mudaram com o tempo: desde ideias até mesmo a própria existência do ser humano como espécie.

9. ASIC**:** Acrônimo de "*Application Specific Integrated Circuit*" (Circuito Integrado de Aplicação Específica), é um *chip* criado especificamente para realizar uma tarefa. No caso do Bitcoin, os *ASICs* foram criados para processar hash SHA-256 e minerar blocos com maior eficiência.

10. Ancapistão: É uma sociedade em que não existe a figura do Estado e os indivíduos podem escolher a qual tipo de governança desejam se submeter. O respeito à propriedade privada e ao livre mercado é a prioridade; serviços como educação, saúde, segurança (pública e privada), tribunais seriam fornecidos por concorrentes privados em vez de coercitivamente pelo Estado.

11. *Bail-in* (Resgate interno): Quando o dinheiro do depositante (sócio ou credor) é usado para tratar a má saúde financeira dos bancos. Por exemplo, quando a Bitfinex hackeada alegava não ter bitcoins para quitar todos os saldos na plataforma e descontou valores dos saldos sacados até a sua recuperação.

12. *Bail-out* (Resgate externo): Quando o recurso externo normalmente “dinheiro público”, é usado para tratar a precária saúde financeira de uma instituição financeira à beira da falência. O governo simplesmente dá dinheiro (na forma de empréstimos, títulos e até em dinheiro) ao banco enfermo para sua sobrevivência.

13. *Backwardation*: ocorre quando o preço futuro é menor do que o preço à vista (*spot*), quando é possível fazer renda fixa em BTC vendendo presente e comprando o futuro. Situação oposta ao ***contango***, em que o valor futuro é maior que o *spot* e é possível fazer *cash and carry*, consolidando renda fixa em dólar.

14. *Betting* (Aposta): É a ação de apostar dinheiro, bens, tempo ou qualquer outra coisa no resultado de algo, como um jogo ou corrida. Em

outras palavras, o ato ou prática de jogar jogos de azar para uma aposta; geralmente em dinheiro.

15. Bit: É uma unidade comum para designar uma subunidade de bitcoin – 1.000.000 de bits é igual a 1 bitcoin. Esta unidade é geralmente mais conveniente para colocar preços em gorjetas, produtos e serviços.

16. Bimetalismo: É o termo econômico para um padrão monetário em que o valor da unidade monetária é definido como equivalente a determinadas quantidades de dois metais, tipicamente ouro e prata, criando uma taxa fixa de troca entre eles.

17. BIP (*Bitcoin Improvement Proposal*): Proposta de melhoria do Bitcoin é um documento para a introdução de recursos ou informações no Bitcoin. O BIP deve fornecer uma especificação técnica concisa do atributo e uma justificativa para a nova proposta de recurso. Esta é a maneira padrão de comunicar ideias, já que o Bitcoin não tem estrutura formal de organização. **O primeiro BIP (BIP 0001) foi enviado por Amir Taaki em 19/08/2011 e descreveu o que é um BIP.**

18. Bitcoin/bitcoin – Bitcoin: Quando grafado em letra maiúscula inicial, é usado para descrever o conceito do sistema ou a rede completa (*software* e *hardware*); bitcoin – em letra minúscula – é usado para descrever a unidade básica com a qual rede denomina movimentação e saldo em contas. É a moeda virtual mundial desenvolvida em código aberto e estrutura descentralizada e difundida pela Internet por indivíduo ou grupo utilizando o pseudônimo "Satoshi Nakamoto". Todas as transações realizadas são armazenadas em um banco de dados *on-line* e seus símbolos são ฿, BTC ou XBT. Atualmente, a menor fração do bitcoin é o centésimo milionésimo, denominado *satoshi*.

19. Bloco (*block*): Um bloco é um registro dentro da *blockchain* que contém e confirma várias transações em espera na *mempool*. Aproximadamente a cada 10 minutos, em média, um novo bloco com transações é anexado à *blockchain* por meio do processo de mineração.

20. *Blockchain*: A *blockchain* é um registro público de transações Bitcoin em ordem cronológica. A *blockchain* é compartilhada entre todos os usuários do Bitcoin. É usada para verificar o registro e a validade de transações Bitcoin e impedir gasto duplo.

21. *Block reward* (Recompensa de bloco**):** Refere-se aos novos bitcoins concedidos pela rede Bitcoin aos seus mineradores elegíveis para cada

bloco minerado com sucesso. Decai em 50% a cada 210.000 blocos, pelo mecanismo chamado *halving* ou *halvening*.

22. Burocracia virtual: Conceito cunhado por Olavo de Carvalho para a classe de indivíduos preparados para ocupar cargos na Administração, mas sem função, "seu único lugar possível na sociedade é no Estado, mas o Estado não tem lugar para eles". Este grupo se diferencia da "geração nem-nem" pela expectativa específica de ingressar em postos do serviço público e é, em grande parte, explicado pelo "educacionismo"[450]. São rejeitados, inativos economicamente, que servem de idiotas úteis no conceito clássico leninista, defendendo interesses de burocratas apenas pela esperança de ocupar algum dia este papel.

23. Captura Administrativa (ou conhecida por Teoria da Captura): É um ponto fundamental do ramo da teoria da escolha pública conhecido como regulação econômica. A captura administrativa é uma forma de corrupção política que ocorre quando uma agência reguladora, criada para agir de acordo com o "interesse público", age em benefício de interesses comerciais ou políticos de específicos grupos de interesse que dominam a indústria ou o setor daquela agência reguladora. A captura do regulador é uma forma de falha do Estado ao criar brecha para firmas ou grupos políticos atuarem de maneira prejudicial ao público, ou seja, produzindo externalidades negativas. Os órgãos são ditos "agências capturadas".

24. Carteira (*wallet*): A carteira Bitcoin é o equivalente a um cofre ou carteira no mundo "legacy" que contém suas chaves privadas e permite que você gaste seus bitcoins efetivamente enviando-os a um novo endereço, geralmente do recebedor.

25. CBDC *(Central Bank Digital Currency)* – são moedas digitais emitidas por bancos centrais, sejam atreladas a uma moeda fiduciária (Yuan digital) ou *stable Commodity* (Petro Venezuelano). São uma etapa para eliminação de moeda alodial (numerário em espécie) e aumento de poderes estatais para aumentar base monetária, maximizando: a) efeito das reservas fracionárias (vez que TODOS os valores estarão depositados em alguma instituição); b) controle estatal (tanto de informação de quem transaciona com quem, como no poder de congelar ou invalidar saldos ou transações); c) capacidade de endividamento dos governos, impossibilitando a elisão ao juro negativo com saque em numerário; e, d) capacidade de políticas de "estímulos ao consumo", com créditos com expiração para uso, como *vouchers* (dinheiro programável). O PIX é uma etapa para a implantação da

CBDC, reduzindo brutalmente privacidade dos usuários em troca de transações mais rápidas e "grátis" – e usam várias soluções comuns em criptos, como pagamentos por *QRcode*. O BCB promete desenvolver soluções de *smart contracts* e até reais digitais *offline* (como *smartcard* usado em transportes).

26. Chave pública *(Public key)*: Um conjunto de números e letras derivado matematicamente de uma chave privada. Você pode compartilhar sua chave pública para poder receber mensagens (com bitcoins) de outros usuários na rede.

27. Chave privada (*Private key*): Uma chave privada é um também conjunto de números e letras, uma combinação única de bytes de informação utilizada para assinar transações. Pense na chave privada como uma senha muito forte. As chaves privadas não devem ser compartilhadas jamais. Qualquer pessoa em posse da sua chave privada pode assinar transações e transferir a posse de seus bitcoins para outra chave privada.

28. *Cypherpunks*: É um grupo informal de pessoas interessadas em criptografia e privacidade.

29. *Cold storage* (Armazenamento a Frio): É uma carteira *off-line* usada para armazenar bitcoins. Com o armazenamento a frio, a carteira digital é armazenada em uma plataforma que não está conectada à Internet, protegendo a carteira contra acesso não autorizado, *hackers* cibernéticos e outras vulnerabilidades às quais um sistema conectado à Internet é suscetível.

30. *Confirmation* (confirmação): Confirmação significa que uma transação foi processada pela rede e é altamente improvável ser revertida. Transações recebem uma confirmação quando são incluídas em um bloco e a cada bloco subsequente. Mesmo uma única confirmação pode ser considerada segura para transações de baixos valores, apesar de que, em valores maiores como US$ 1.000, faz sentido esperar por 6 confirmações ou mais. Cada confirmação reduz exponencialmente o risco de uma transação ser revertida.

31. *Core developers* (Desenvolvedores principais): São os líderes do projeto. Propõem, avaliam e implementam melhorias, corrigem erros e estabelecem uma visão para o projeto, quando apropriado.

32. *Crypto*/cripto: Significa criptografada, oculta. Criptografia é o estudo de ocultar as coisas, a criptomoeda é a moeda criptografada.

33. Criptografia: A criptografia é o ramo da matemática que nos deixa criar provas matemáticas que fornecem um alto nível de segurança. Já sendo utilizada em comércio *on-line* e bancos. No caso do Bitcoin, a criptografia é utilizada para fazer com que seja impossível para qualquer um gastar fundos da carteira de outro usuário ou corromper a *blockchain*. Também pode ser utilizada para encriptar uma carteira, de modo que ela não pode ser utilizada sem uma senha.

34. *Crowdfunding* (Financiamento coletivo): Consiste na obtenção de capital para financiar um determinado projeto de interesse coletivo, em geral com participação de pessoas físicas interessadas na iniciativa.

35. Curva de Laffer: É uma representação teórica que afirma que, se as taxas de impostos aumentam acima de um certo nível, as receitas fiscais podem realmente cair, porque as taxas de impostos mais altas desencorajam as pessoas a pagar. Da mesma forma, a Curva de Laffer afirma que o corte de impostos poderia, em teoria, levar a receitas fiscais maiores.

***36. DAO* (*Decentralized Autonomous Organization*):** É uma organização cujas regras são especificadas através de programas de computador conhecidos como contratos inteligentes, os quais são executados e validados por uma *blockchain*.

37. Descentralizado: Manter um conceito fora do controle de uma única entidade e fazer com que a população geral trabalhe em conjunto como fator de controle.

38. Dissonância Cognitiva: Segundo a Teoria da Dissonância Cognitiva de Leon Festinger (1957), ocorre o fenômeno quando um indivíduo possui opiniões ou comportamentos incompatíveis com suas crenças - havendo elementos cognitivos sem coerência. Exemplo simples vem de a "Raposa e as uvas" de Esopo, em que a Raposa, por desejar algo inatingível, passa a criticar o objeto de desejo para reduzir sua dissonância.

39. Dividendo demográfico: Período, normalmente entre 20 e 30 anos, durante o qual as taxas de fertilidade e mortalidade caem e as populações têm o crescimento anormal na produtividade econômica devido ao pico na proporção de pessoas em idade produtiva (no Brasil, estima-se que o ápice da razão de dependência ocorra entre 2019 e 2022). Inverno demográfico: fenômeno percebido quando a taxa de natalidade se mantém em queda e a taxa de mortalidade mantém-se em níveis baixos. Isso tem como consequência o envelhecimento da população e a limitação das possibilidades de crescimento econômico. Segundo dados oficiais (IBGE),

as projeções indicam taxas de fecundidade em quedas sucessivas (6,21 em 1960; 4,07 em 1980; 1,81 em 2012; 1,74 em 2014 e projeção de 1,69 para 2016).

40. Dilema de Triffin (paradoxo de Triffin): É o conflito de interesses econômicos que surge entre os objetivos domésticos de curto prazo e os objetivos internacionais de longo prazo para países cujas moedas servem como moedas de reserva global. Esse dilema foi identificado na década de 1960 pelo economista belga-americano Robert Triffin, que apontou que o país cuja moeda é a moeda de reserva global, que as nações estrangeiras desejam manter, deve estar disposto a fornecer ao mundo um suprimento extra de sua moeda para atender à demanda mundial por essas reservas cambiais, levando a um *déficit* comercial. Para Robert Triffin, o sistema de Bretton Woods continha uma falha inerente e potencialmente fatal, ou seja, sua dependência em relação ao dólar, que deveria, conforme havia sido decidido em Bretton Woods, manter seu padrão-ouro.

41. *DYOR (Do Your Own Research*): Significa "faça sua própria pesquisa" e é uma frase comum utilizada na internet para que os usuários não caiam em desinformação, a frase se tornou muito usada por entusiastas de criptomoedas.

42. *Early adopter*: Alguém que é uma das primeiras pessoas a começar a usar um novo produto, especialmente uma nova peça de tecnologia.

43. Empréstimo Colateralizado: É um ativo que é dado como garantia de pagamento para uma obrigação de dívida. Por exemplo, no caso de uma hipoteca, o imóvel serve como colateral do empréstimo e, no mercado de criptomoeda, deixa uma quantia em crypto como garantia. Desta forma, o banco ou plataforma *crypto* possui uma garantia em caso de não cumprimento do devedor.

44. Efeito Cantillon: Os primeiros a receber o dinheiro recém-criado por um Banco Central veem sua renda subir, enquanto os últimos a receber o dinheiro veem seu poder de compra declinar.

45. Efeito *Dunning-Kruger*: Explica por que pessoas de baixo QI e conhecimento se sentem confiantes e capazes de emitir opiniões, viés cognitivo de ilusória superioridade.

46. Efeito Rede: É um fenômeno pelo qual um número crescente de pessoas ou participantes melhora o valor de um bem ou serviço. A Internet é um exemplo do efeito de rede. Inicialmente, havia poucos usuários na Internet, uma vez que era de pouco valor para qualquer pessoa fora do

exército e para alguns pesquisadores. No entanto, à medida que mais usuários obtinham acesso à Internet, eles produziam mais conteúdo, informações e serviços. O desenvolvimento e aprimoramento de *sites* atraíram mais usuários para se conectarem e negociarem entre si. À medida que a Internet experimentava aumento no tráfego, ela oferecia mais valor, levando a um efeito de rede.

47. Efeito Lindy: É o conceito de que o futuro da expectativa de vida de algumas coisas não perecíveis, como uma tecnologia ou uma ideia, é proporcional à sua idade atual, de modo que cada período adicional de sobrevivência implica uma maior expectativa de vida restante. Logo, quanto mais antigo algo for, mais tempo provavelmente existirá no futuro. De acordo com o Efeito Lindy, como o bitcoin existe há cerca de 10 anos, podemos esperar que ele continue por mais 10 anos. A cada ano a mais que ele sobrevive, mais tempo podemos esperar que ele esteja por aí no futuro. Como Taleb nos diz, a robustez de algo é proporcional à sua vida. Quanto mais tempo sobrevive, maior é a probabilidade de continuar a sobreviver.

48. Endereços: Equivalente à conta de um banco, informação necessária para envio de bitcoin, derivado da chave pública. **Existem 3 tipos de endereços no Bitcoin** Bech32 (*Segwit* Nativo) que começam com bc1. **Ex.:** bc1qar0srrr7xfkvy998745ydnw9an59gtzzwf9mdq. **Situação:** Compatível somente com carteiras que aceitam *segwit*. Dessa forma, uma carteira antiga pode não reconhecer fundos enviados a partir desse endereço. **Obs.:** Oferece as menores taxas possíveis. **Endereços:** *P2SH (Pay-to-Script-Hash*, *Segwit*). **Início:** Começam com 3. **Ex.:** 3K965KmP1Z73CnmQviecrnyiWrnqRhWXuA. **Situação:** Endereço de transição: Melhor opção para a maior parte dos usuários por ser compatível com todas as *wallets*. **Obs.:** Baixas taxas de transação. **Endereços:** ***P2PKH Legacy*** **(*Pay-to-PubkeyHash*, não *segwit*). Início:** Começam com 1. **Ex.:** 1OvyeornyiWrnqRhWXuAK965KmP1Z73CNm. **Situação:** Endereço antigo: Endereço compatível com todas as *wallets*.

49. *Exchanges* (corretoras): Uma “corretora” de criptomoedas, ou uma troca de moeda digital, é uma empresa que permite aos clientes negociarem criptomoedas ou moedas digitais por outros ativos, como moeda fiduciária convencional ou outras moedas digitais.

50. *Equity tokens* (*token* de patrimônio): Os *equity tokens* funcionam mais como um ativo de *stock asset.* Em outras palavras, os detentores de *tokens* de patrimônio possuem alguma forma de propriedade em seus

investimentos. Seus *tokens* representam quanta porcentagem de propriedade eles realmente possuem. Na maioria dos casos, os *tokens* de patrimônio representam um ativo, propriedade ou empreendimento de terceiros. Os *equity tokens* vêm em muitas formas: *Stocks*, Contratos Futuros, Opções, *Tokenized Real Estate* e *Tokenized Ventures.*

51. Efeito Gell-Mann: Em um discurso em 2002, Crichton cunhou o termo efeito da amnésia de Gell-Mann. Ele usou esse termo para descrever o fenômeno de especialistas acreditarem em artigos de notícias sobre tópicos fora de suas áreas de especialização, mesmo depois de reconhecerem que artigos dentro de suas áreas de especialização escritos na mesma publicação estão cheios de erros e mal-entendidos. Ele explica a ironia do termo dizendo que surgiu "porque uma vez eu discuti isso com Murray Gell-Mann, e ao mencionar um nome famoso, dou maior importância a mim mesmo e ao efeito do que o faria de outra forma."

52. *Faucets* (Torneiras): Uma torneira de bitcoin é um sistema de recompensa, na forma de um *site* ou aplicativo, que distribui recompensas na forma de um *satoshi*, que é um centésimo de um milionésimo de BTC, para os visitantes reivindicarem em troca de concluir um *captcha* ou tarefa, conforme descrito pelo *site*.

53. *Fork (soft fork e hard fork):* *Fork* é uma ramificação de uma rede de moedas, pode ser uma atualização ou nova versão. Se for retrocompatível, é *soft fork*; se não for retrocompatível, é *hard fork* – como os *forks* que resultaram no *bitcoin cash, bitcoin gold* e demais novas moedas que reconheceram blocos do bitcoin até certo ponto rodando seu próprio cliente incompatível (com suas próprias regras) depois.

54. *Fees*: O valor pago a um minerador para incluir uma transação em um bloco.

55. Gasto duplo: É uma possível causa de falha de sistemas de criptomoedas. O gasto duplo acontece quando um usuário consegue gastar as mesmas moedas digitais mais de uma vez. Diferentemente de moedas físicas, arquivos digitais podem ser duplicados, logo, o ato de gastar uma moeda digital não implica uma transferência de posse da mesma para outra pessoa. Portanto, é necessário que outros meios sejam utilizados para prevenção contra o gasto duplo.

56. Generais Bizantinos: Em computação, o Problema dos Dois Generais é um experimento mental para ilustrar as armadilhas e desafios de

planejamento na tentativa de coordenar uma ação através da comunicação sobre um ato não confiável.

57. *Gold Standard* (padrão-ouro): É um sistema monetário no qual a unidade de conta econômica padrão é baseada em uma quantidade fixa de ouro. O padrão-ouro foi amplamente utilizado no século XIX e no início do século XX. A maioria das nações abandonou o padrão-ouro como base de seus sistemas monetários durante o século XX, embora muitos ainda mantenham reservas de ouro substanciais.

58. Geração nem-nem: O termo refere-se à população jovem fora do mercado de trabalho e de instituições educacionais.

59. *Halving (halvening):* É um ajuste que ocorre na rede do Bitcoin e que reduz pela metade a recompensa dos mineradores, o que tem como consequência um corte na oferta de novas criptomoedas. E isso garante a característica deflacionária deste ativo.

60. *Hash/hashing:* Também conhecido como ID da transação ou txID, é um identificador único que pode ser usado em qualquer explorador de blocos para buscar por detalhes públicos de uma transação específica. Toda transação feita *on-chain* tem um *hash* único composto por vários caracteres alfanuméricos. Todo *hash* é único e derivado das informações da transação. Uma função *hash*, como as funções *hash* usadas para criar os diferentes tipos de endereços, é um algoritmo que mapeia dados de comprimento variável e os converte em dados de comprimento fixo. Os valores retornados por uma função *hash* são chamados de *hashes* e eles servem para compactar dados e assegurar a integridade dos dados transmitidos.

61. *Hashrate* (taxa de *hash*): A taxa de *hash* é a unidade de medida do poder de processamento da rede Bitcoin. A rede Bitcoin deve fazer operações matemáticas intensivas para fins de segurança. Quando a rede atinge uma taxa de *hash* de 10 Th/s, significa que ela pode processar 10 trilhões de cálculos por segundo.

62. *Hash*: Uma função que mapeia dados de comprimento variável em dados de tamanho fixo. Usado para identificar transações, blocos, calcular endereços e minerar blocos.

63. *Hodl* (*holdlers*): Um erro de escrita cometido por um usuário do pioneiro fórum Bitcointalk durante a *bull run* de 2013, que escreveu a palavra *Holding* (segurar) de forma errada, *Hodling*. Surgiu então o verbo "*to hodl*". *Hodler* é uma pessoa que não vende e segura seus bitcoins independente se o preço subir ou cair.

64. *Hedge* (Cobertura): É uma estratégia de proteção para os riscos de um investimento, que neutraliza a posição comprada ou vendida contra o risco de grandes variações de preço de um determinado ativo. Ao fazer uma operação de *hedging*, o investidor tem como objetivo eliminar a possibilidade de perdas futuras.

65. *Hard money*: Moeda forte, moeda com boa cotação cambial.

66. *Hardware Wallet:* Um dispositivo relativamente seguro e prático (como *Ledger, Keepkey* e *Trezor*) para armazenar e assinar transações, protegendo as chaves privadas de transações.

67. Hiperbitcoinização: Esse fenômeno pode ser mais observado primeiramente em economias emergentes e subdesenvolvidas. O bitcoin se torna(rá) um refúgio seguro frente aos descompassos do Estado que causa crises financeiras: colapso das moedas nacionais, hiperinflação, colapso das dívidas nacionais.

68. *HFSP (Have fun staying poor):* A frase significa "Divirta-se ficando pobre. Frase que virou um "meme" como uma resposta a alguém que acabou de vender bitcoin ou disse que nunca consideraria comprar bitcoin.

69. *ICO* (*Initial coin offering*): Uma oferta inicial de moedas (*ICO*) é o equivalente do setor de criptomoedas a uma oferta pública inicial (IPO). As *ICOs* funcionam como uma maneira de arrecadar fundos, em que uma empresa que busca arrecadar dinheiro para criar uma nova moeda, aplicativo ou serviço lança uma *ICO*. Os investidores interessados podem comprar a oferta e receber um novo *token* de criptomoeda emitido pela empresa. Esse *token* pode ter alguma utilidade no uso do produto ou serviço que a empresa está oferecendo ou pode representar apenas uma participação na empresa ou no projeto.

70. *IOUs* ("*I owe you*"): É geralmente um documento informal que reconhece uma dívida. Um *IOU* difere de uma nota promissória, pois um *IOU* não é um instrumento negociável e não especifica termos de reembolso, como o horário do reembolso. Os *IOUs* geralmente especificam o devedor, o valor devido e, às vezes, o credor.

71. Impersonificação: Deixar de possuir qualidades, características ou aspectos de pessoa; fazer com que alguém ou si mesmo deixe de possuir qualidades pessoais. Etimologia (origem da palavra *impersonificar*). Im + personificar. (Dicionário *on-line* de Português).

***72. KYC* ("*know your customer*"):** política financeira de exigir identificação do cliente, apresentação de documentos e até com

reconhecimento facial, de voz e de digitais.

73. Lei de Gresham: A Lei de Gresham resume-se na seguinte oração: É um princípio econômico que diz que uma moeda sobrevalorizada (tem um valor determinado por uma autoridade monetária acima do de mercado) expulsa uma moeda subvalorizada (tem um valor determinado pela mesma autoridade abaixo do de mercado). Por exemplo, nos padrões bimetálicos, a prata circulava mais e o ouro era mais entesourado; ou, como hoje na Venezuela, em que os bolívares têm alta velocidade e os dólares são guardados como reserva de valor.

74. Lei de Amara: O cientista Roy Charles Amara definiu uma regra que encoraja todos a pensar um pouco mais sobre a tecnologia. A lei diz que “Tendemos a superestimar o efeito de uma tecnologia no curto prazo e a subestimar seu efeito no longo prazo”. Ou seja, temos a tendência de ficar extremamente entusiasmados com as novas tecnologias e nossas expectativas inicialmente superam a realidade. Porém, eventualmente, essa dinâmica muda e começamos a subestimar o impacto que uma tecnologia terá.

75. Lei de Metcalfe: A lei de Metcalfe afirma que o efeito de uma rede é proporcional ao quadrado do número de usuários conectados no sistema (n^2). A lei caracteriza muitos dos efeitos de rede de tecnologias de comunicação e redes como a Internet, redes sociais e a *World Wide Web* e também a rede Bitcoin (com base no número de usuários ativos).

76. Lei de Wagner: Também conhecida como a lei do aumento da despesa do Estado. A lei de Wagner sugere que um Estado Social evolui de capitalismo de livre mercado, devido ao fato de a população exigir cada vez maiores serviços sociais. Os neokeynesianos e os socialistas muitas vezes exortam os governos a imitar Estados de Bem-Estar modernos, como a Suécia. A despesa pública aumenta constantemente, mostrando uma tendência ascendente. Tal lei prevê que o desenvolvimento de uma economia industrial será acompanhada por um aumento da percentagem da despesa pública no Produto Interno Bruto: “O advento da sociedade industrial moderna resultará no aumento da pressão política para o progresso social e aumento da provisão para créditos de consideração social pela indústria.”

77. Lei de Michels ou Lei da Oligarquia: afirma que democracia e organização de grande escala são incompatíveis, confirmando a falsidade da "Teoria do interesse público".

78. Lei de Moore: É uma observação e projeção de uma tendência histórica relacionada à indústria de microchips e processamento de computadores. Foi observada por Gordon E. Moore, e consiste na previsão de que o número de transistores dos chips teria um aumento de 100%, pelo mesmo custo, a cada período de 18 meses.

79. Lei de Gall (*Gall's Law*): "Um sistema complexo que funciona invariavelmente evoluiu de um sistema simples que funcionava. A proposição inversa também parece ser verdadeira: um sistema complexo projetado do zero nunca funciona e não pode ser feito para funcionar. Você tem que começar de novo, começando com um sistema simples de trabalho." John Gall

Outra lei que o Bitcoin respeita é a *Gall's Law.* O Bitcoin é muito simples. Ele minimiza o número de variáveis dinâmicas. Novos sistemas complexos são incrivelmente difíceis de projetar do zero.

Um processo é bom quando não se trata de construir sistemas complexos do zero. Comece com um sistema simples que funcione e aprimore-o. Como alternativa, pegue um conjunto de subsistemas que estão funcionando (pequenos) e os componha, mas certifique-se de que a composição em si não se torne complexa, pois isso também não funcionará. Desenvolva iterativamente em pequenos passos e frequentemente certifique-se de que o resultado ainda está funcionando.

80. *Legacy System* (sistema legado): O termo "sistema legado" descreve um sistema antigo que permanece em operação em uma organização.

81. *Long e Short*: É uma estratégia que consiste em uma operação casada, na qual um investidor mantém uma posição vendida em um ativo (ação/criptomoeda) e comprada em outro no intuito de obter um residual financeiro da operação quando liquidá-la. Esta operação permite alavancagem financeira, pois é lastreada com margens de garantia.

82. *Lending / Marging lending* (empréstimo): O empréstimo de criptomoeda é a situação em que os investidores podem usar seus ativos cripto como garantia para obter um empréstimo fiduciário ou *stablecoin*, enquanto os credores fornecem os ativos necessários para o empréstimo a uma taxa de juros acordada.

83. Mineração: é o processo de utilização de computadores para realizar cálculos matemáticos para confirmar as transações da rede Bitcoin e aumentar a segurança. Como recompensa por seus serviços, os mineradores de bitcoin podem receber as taxas das transações confirmadas, além de

novas moedas criadas em cada bloco. A mineração é um mercado especializado e competitivo em que os benefícios são partilhados de acordo com o número de cálculos que são realizados. Nem todos os usuários bitcoin são mineradores e não é uma maneira fácil de ganhar dinheiro.

84. *Miner fee* (Taxa de mineração) / *Trasaction fee* (Taxa de transação): São pequenas quantidades de bitcoin concedidas para incentivar os mineradores de bitcoin a confirmar transações de bitcoin. Os mineradores de bitcoin são peças importantes que confirmam e protegem as transações na rede de Bitcoin. As taxas dos mineradores pagam aos mineradores pelo serviço que prestam.

85. *Mempool*: O grupo de transações esperando para serem incluídas em um bloco por um minerador.

86. Mercado futuros: Um contrato de futuros é um acordo legal para comprar ou vender um determinado ativo sendo ele commodity ou título a um preço predeterminado em um momento específico no futuro.

87. *Multisig*: A assinatura múltipla é uma configuração de carteira que pode exigir mais de uma chave privada para autorizar uma transação.

88. Moeda fiduciária (*Fiat*): É a moeda legal de qualquer país em que é impressa e emitida pelo governo via Banco Central. Moeda fiduciária é qualquer título não conversível, ou seja, não é lastreada a nenhum metal (ouro, prata) e não tem nenhum valor "intrínseco". Seu valor advém da confiança que as pessoas têm em quem emitiu o título.

89. Monerização: monerizar é aumentar fungibilidade e privacidade (do *token* ou da rede), saldos de bitcoin na *liquid/lightning* seriam "monerizados", ou o próprio Bitcoin estaria se aproximando aos atributos do monero ao adotar *Taproot* e outras melhorias de fungibilidade e privacidade.

***90. Network computer* (Rede de computadores):** Ou Rede de dados, na informática e na telecomunicação é um conjunto de dois ou mais dispositivos eletrônicos de computação (ou módulos processadores ou nós da rede) interligados por um sistema de comunicação digital (ou link de dados), guiados por um conjunto de regras (protocolo de rede) para compartilhar entre si informação, serviços e, recursos físicos e lógicos.

***91. Node* (nó):** Um *node* é um participante ativo e soberano da rede *P2P* do Bitcoin. Existem dois tipos de *node*: *full node* (nó completo), um nó que

carrega uma cópia completa da *blockchain*, e *pruned node* (nó cortado), um nó que tem apenas os últimos blocos da rede bitcoin. Ambos os nodes validam transações e propagam as transações pela rede, além de ter *mempool*. A única diferença é que o nó *pruned* não tem os blocos mais antigos da rede para ajudar na sincronização inicial dos blocos por novos nós entrando na rede.

92. Noob/newbie**:** calouro, iniciante.

93. NGU (Number go Up) Technology: Foi cunhado pelo famoso *bitcoiner* Pierre Rochard no twitter: “Bitcoin é a tecnologia NGU mais avançada do mundo.” Isso quer dizer que os recém-chegados elevam a quantidade de usuários utilizando a rede bitcoin, ao passo que o preço do ativo também aumenta. A tecnologia *Number Go Up* expandido a sua abordagem também se refere a extrema escassez do bitcoin e a incapacidade de copiar seu efeito rede, isso resulta no aumento do preço do Bitcoin ao passo que outros atributos também aumentam como: quantidade de nós Bitcoin ativos; *Hashpower*; colaborações dos desenvolvedores; empresas provendo produtos e serviços; empregos gerados em todo ecossistema Bitcoin; números de transações; cobertura da mídia e FOMO; financiamento em projetos e desenvolvimento do Bitcoin.

94. Open source**:** *Software* de código aberto é aquele em que o código-fonte é disponibilizado e licenciado com uma licença de código aberto na qual o direito autoral fornece o direito de estudar, modificar e distribuir o *software* de graça para qualquer um e para qualquer finalidade.

95. On-chain (dentro da cadeia): As transações dentro da cadeia referem-se às transações de criptomoeda que ocorrem na *blockchain* - isto é, nos registros do *blockchain*, e permanecem dependentes do Estado da *blockchain* para sua validade. Todas essas transações em cadeia ocorrem e são consideradas válidas apenas quando da *blockchain* é modificado para refletir essas transações nos registros/livro de razão público.

96. Off-chain (fora da cadeia): As transações fora da cadeia referem-se às transações que ocorrem em uma rede de criptomoedas que movem o valor para fora da *blockchain*. Devido ao seu custo zero/baixo, liquidação imediata e maior anonimato, as transações fora da rede estão ganhando popularidade, especialmente entre grandes *exchanges*.

97. OTC – Over The Counter **(Mercado Balcão):** É a situação em que investidores profissionais, fundos, empresas e pessoas compram e vendem um ativo em grandes quantidades fora da *Exchange*.

***98. P2P* (*Peer-to-peer*):** É uma arquitetura de redes de computadores em que cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central. No caso do Bitcoin, a rede é construída de modo que cada utilizador transmita as transações de outros.

99. Pirâmides / *Ponzi Scheme* (esquema Ponzi): É um esquema com operação fraudulenta sofisticada de investimento do tipo esquema em pirâmide que envolve a promessa de pagamento de rendimentos anormalmente altos aos investidores à custa do dinheiro pago pelos investidores que chegarem posteriormente, em vez da receita gerada por qualquer negócio real. No Brasil, até a participação é criminalizada desde a Lei 1.521/51, art. 2, IX (pichardismo e equivalentes).

100. Profecia autorrealizável: Prognóstico que provoca sua própria concretização. Previsão que influencia o comportamento das pessoas de modo que acaba se realizando. Conceito de Robert Merton (1949). Muitas vezes é causado pelo “efeito manada”, quando grupos se comportam de maneira semelhante sem organização planejada, seguindo o padrão da “massa crítica” - número mínimo de adotantes para sustentar ação.

101. *Proof of Brain* (prova de cérebro): medida de quanto de inteligência há em um ambiente ou projeto, aferida pela qualidade dos envolvidos e número e qualidade das contribuições nos repositórios.

102. *PoW (Proof of Work)*: Refere-se a uma porção dos dados que é difícil (consome muitos recursos e tempo) de ser produzida e extremamente fácil de verificar se atende alguns requisitos predeterminados. Produzir prova de trabalho pode ser um processo aleatório com baixa probabilidade de acerto, para que muita tentativa e erro (força bruta) seja requerida em média antes que uma prova seja gerada.

103. *PoS (Proof of Stake):* Prova de participação, normalmente com saldo vinculado ao nó.

104. *Pump and dump:* É um esquema de manipulação que envolve o aumento artificial do preço de um ativo por meio de declarações positivas falsas e enganosas (muitas vezes através de grupos do *telegram* ou relatórios de investimento), a fim de vender o ativo por preço mais alto (e algumas vezes recomprar depois de divulgação de notícias negativas, igualmente falsas ou fabricadas).

105. Preferência temporal: A preferência temporal é uma teoria em economia que trata a respeito da escolha de investimento e consumo de

bens em relação ao tempo. Os indivíduos estão sujeitos à passagem do tempo. Suas existências são finitas, seus corpos e mentes decaem. O tempo, portanto, é um fator escasso e, como tal, os indivíduos precisam economizá-lo.

106. Baixa preferência: Quando você possui visão de longo prazo. Ao não desfrutar de um bem no presente, a pessoa está disposta a algum sacrifício (poupar é sempre um ato de sacrifício) para adiar o usufruto desses bens no presente. Por isso, ao consumir pouco, a pessoa tem a preferência temporal baixa, nisso se permite que haja mais bens disponíveis para ser emprestados e aplicados em processos de investimento. Uma preferência temporal baixa gera uma maior abundância de bens livres para ser emprestados.

107. Alta preferência: Quando a pessoa possui visão de curto prazo. A pessoa se torna uma consumista, voltada sempre ao tempo presente e avessa à poupança. A escassez de capital é a consequência natural da alta preferência temporal das pessoas, traduzindo-se em um alto preço (juros) cobrado pelo uso do pouco capital que ainda resta.

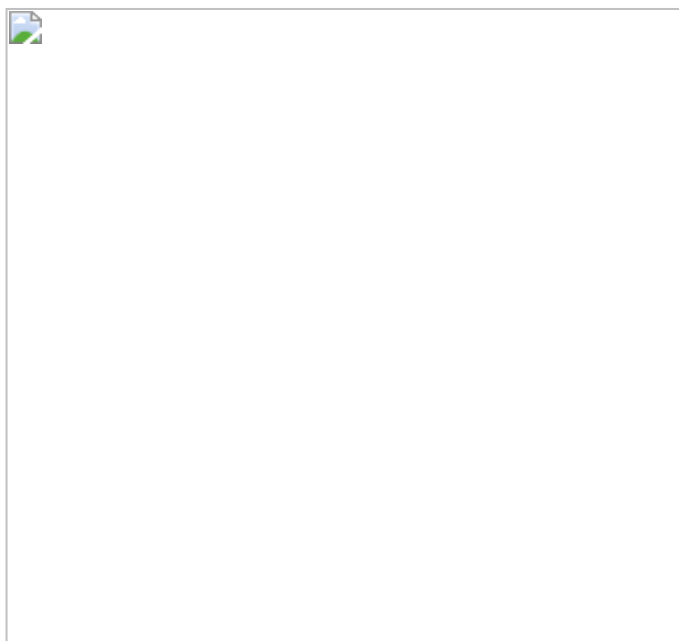
108. Ponerologia Política: É o estudo do mal, do grego *poneros* (malícia, maldade), é a ciência da natureza do mal adaptada a propósitos políticos. O termo foi cunhado pelo psiquiatra polonês Andrzej M. Lobaczewski, que estudou como os psicopatas influenciam no avanço da injustiça e como abrem caminho para o poder na política.

109. Problema de Olson (A Lógica da Ação Coletiva): A tese básica deste livro é a de que "mesmo que todos os indivíduos de um grupo grande sejam racionais e centrados em seus próprios interesses, e que saiam ganhando se, como grupo, agirem para atingir seus objetivos comuns, ainda assim eles não agirão voluntariamente para promover esses interesses comuns e grupais" (Olson, 1999, p. 14).

110. *Paper wallet*: Uma carteira *off-line* de armazenamento frio (*cold storage*), em que a chave privada é impressa em um pedaço de papel para armazenamento *off-line*. Era considerada uma das maneiras mais seguras de armazenar chaves privadas antes da criação de soluções de *hardware* e da implementação do *backup* a partir de *seed* (mnemônicos).

111. *Quantitative easing* (alívios quantitativos): A flexibilização quantitativa (QE) é uma forma de política monetária não convencional, na qual um Banco Central compra títulos de longo prazo no mercado aberto, a fim de aumentar a oferta de moeda e incentivar empréstimos e

investimentos. A compra desses títulos acrescenta mais dinheiro à economia e também serve para diminuir as taxas de juros, oferecendo títulos de renda fixa. Também expande o balanço do Banco Central. Quando as taxas de juros de curto prazo são iguais ou próximas a zero, as operações normais de mercado aberto de um banco central, que têm como alvo as taxas de juros, não são mais eficazes. Em vez disso, um Banco Central pode direcionar quantidades especificadas de ativos para compra. A flexibilização quantitativa aumenta a oferta de dinheiro comprando ativos com reservas bancárias recém-criadas, a fim de fornecer mais liquidez aos bancos.

112. Saylorização: processo de empresas abertas usarem juro negativo para comprarem bitcoin alavancado em vez de fazer recompra de ações, em processo de ataque especulativo contra *fiats*, fazendo até mesmo investidores de índices como SP500 se expor marginalmente a bitcoin.

113. *Smart contracts* (contratos inteligentes): É um contrato de execução automática com os termos do contrato entre comprador e vendedor sendo gravados diretamente em linhas de código. O código e os acordos nele contidos existem em uma rede *blockchain* descentralizada e distribuída. O código controla a execução e as transações são rastreáveis e irreversíveis. Os contratos inteligentes permitem que transações e acordos confiáveis sejam realizados entre partes anônimas e díspares, sem a necessidade de uma autoridade central, sistema legal ou mecanismo de

execução externo. Embora a tecnologia *blockchain* venha a ser pensada principalmente como a base do bitcoin, ela evoluiu muito além de sustentar uma criptomoeda.

114. *Slippage*: Refere-se à diferença entre o preço esperado de uma negociação e o preço pelo qual a negociação é executada. A derrapagem pode ocorrer a qualquer momento, mas é mais prevalente durante os períodos de maior volatilidade quando as ordens de mercado são usadas. Também pode ocorrer quando uma grande ordem é executada, mas não há volume suficiente no preço escolhido para manter o *spread* de compra / venda atual.

115. *Satoshi/sats*: A menor unidade divisível de um bitcoin. Cada unidade de bitcoin é composta de 100 milhões de *satoshis* (8 casas decimais). 1 *satoshi* (1 sat) = 0,00000001 bitcoin / 1 bitcoin = 100.000.000 de sats.

116. *Scam*: É um esquema fraudulento armado intencionalmente para enganar uma pessoa ou grupo de pessoas com objetivo de roubar dinheiro.

117. *Shitcoins*: É um termo pejorativo usado para descrever uma criptomoeda que se tornou inútil. É uma criptomoeda sem propósito, valor ou futuro.

118. Shitcoinheiro: Indivíduos que, por ignorância ou malícia, acumulam e/ou promovem tokens digitais sem valor. Muitos shitcoinheiros carecem de conhecimento nas áreas da economia austríaca, modelos de camadas de escala de protocolo, teoria dos jogos e ética. Muitos são propensos a explosões emocionais quando expostos à razão ou a perguntas difíceis sobre seus portfólios diversificados. Os passatempos incluem divertir-se se mantendo pobre e criar definições para maximalistas de Bitcoin no Urban Dictionary.

Steve ignorou o Bitcoin por anos e sente que perdeu o barco, apesar de seus amigos bitcoinheiros tentarem fazer com que ele acumulasse sats repetidamente. Para recuperar o tempo perdido, ele pulou na Coinbase e comprou todas as moedas de baixa capitalização na esperança de que um dia fosse o "próximo" Bitcoin. Steve é um cretino total. (By: BTC Sessions August 16, 2021).

119. *Sound money* (Dinheiro sonante): É aquele que não está sujeito a apreciação ou depreciação repentina do poder de compra no longo prazo, auxiliado por mecanismos de autocorreção inerentes a um sistema de livre mercado.

120. *Stablecoins:* É uma classe de criptomoedas que tenta oferecer estabilidade de preços e é garantida por um ativo de reserva (dólar, euro, ouro etc.). Os *Stablecoins* ganharam força ao tentar oferecer o melhor dos dois mundos, o processamento instantâneo e a segurança ou privacidade dos pagamentos de criptomoedas e as avaliações estáveis sem volatilidade de moedas fiduciárias.

121. Teoria das Escolhas Públicas: A escolha pública ou Teoria da Escolha Pública é um ramo da teoria econômica em que os conceitos da economia de mercado são aplicados à política e aos serviços públicos. Assim, na ciência política, a escolha pública critica a visão romântica de que o político é um servidor altruísta do interesse público em geral, substituindo-a por uma abordagem mais consentânea com o comportamento humano. Em vez de conceder aos políticos um tratamento especial, a escolha pública os trata como meros agentes humanos que priorizam a satisfação do seu próprio interesse.

121. *Testnet*: É uma rede separada com um *design* quase idêntico ao da rede Bitcoin para que os desenvolvedores possam testar melhorias e inovações sem colocar *satoshis* de verdade em risco.

122. UTXO: Acrônimo de "*Unspent Transaction Output*" (saída de transação não gasta) é uma moeda de bitcoin que pode ser usado como *input* (entrada) para ser gasto em transações futuras. Basicamente, é como os bitcoins que você possui e pode gastar são chamados dentro da rede Bitcoin. O saldo de uma carteira Bitcoin, por exemplo, é a soma de UTXOs controladas pelas chaves privadas daquela carteira.

123. xPub: Significa *"Extended Public Key"* (chave pública estendida). As chaves xPub são úteis porque o Bitcoin emprega o conceito de saídas de transação não gastas (UTXOs) em endereços de retorno. É a chave que gera todos os endereços, assim, podem-se obter todos os dados da sua carteira, transações anteriores e futuras. Mesmo que signifique "chave pública estendida", esta chave deve permanecer privada e nunca ser compartilhada.

124. *Welfare State* (Estado de bem-estar social): O Estado de bem-estar social, ou Estado-providência, ou Estado social, é um tipo de organização política, econômica e sociocultural que coloca o Estado como agente da promoção social e organizador da economia.

[1] Maximalistas - como *shitcoins* são testes de QI e BTC teste de fé no *legacy*: https://bit.ly/3Asikbq

[2] *Bitcoin Finance (BiFi)* vai ter *DeFi* e *CeFi*: https://atomic.finance/blog/a-sound-finance-manifesto/

[3] *RSK Network:* https://www.rsk.co/ / *Sidechain RSK - Convidada Solange Gueiros*: https://bit.ly/3sNzyfX

[4] *Liquid Network:* https://liquid.net/ / Tudo sobre a *Liquid*: https://bit.ly/38b3kC2

[5] *Lightning Network:* https://lightning.engineering/ / *LN* para iniciantes: https://bit.ly/2UTCECQ

[6] Exemplos do que estará no próximo volume: futurologia, descrição de conceitos de singularidade; disrupção; anapistão e justiça privada; mudança exponencial; economia da abundância; *digital dividel; seasteading* e *Citadel*, assim como, mecanismos e problemas de *smart contracts* (passados, atuais e potenciais) — *como os mercados decentralizados de apostas de morte; stables colateralizadas* como DAI do *maker DAO;* plataformas de apostas e serviços financeiros descentralizados e seus problemas intrínsecos; esquemas fraudulentos elaborados através de manipulação de mercado, *ICO*s ou *forks* maliciosos; consequências materiais e morais da hiperbitcoinização; natureza jurídica e econômica de *tokens* e minúcias das estratégias de *compliance;* gestão de riscos (inclusive com produtos criados com derivativos e futuros) e planejamento tributário e sucessório, ficam para o próximo volume.

[7] Comunismo é o polilogismo: https://bit.ly/3xa1ThS (arquivado: http://archive.today/hxCYX). E o progressismo atual depende de *behavioural bilingualism* (espécie de paralaxe cognitiva) para desmoralização e dessensibilização, como nas políticas de forçar uso de focinheira insalubre de pano que aumenta fómites e de confinamento de inocentes sem qualquer fundamento lógico ou empírico: https://bit.ly/2TyEvvV Mises denominava essa patologia "Complexo de Fourier": https://bit.ly/3dHN7Hz

[8] *Imposto = Roubo*: https://bit.ly/2SLF19H (arquivado: http://archive.today/8MLkN).

[9] *Legacy* é o sistema, em tecnologia, obsoleto, mas ainda operando, como a telefonia fixa.

[10] *Day Trading Bitcoin: Why 95% of Traders Lose Money and Fail*: https://bit.ly/3gnE1A9 (arquivado: https://archive.vn/DfLO1).

[11] Preço médio é *DCA* (*dollar cost averaging*), veja quanto teria hoje comprando 1 ou 10 ou US$100 por semana ou mês em BTC: https://dcabtc.com

[12] *Any Monkey Can Beat The Market:* https://bit.ly/3v7SVjx (arquivado: https://archive.vn/wYyJ8).

[13] Desde o Antigo Testamento, já se sabia que todos os retornos são proporcionais a esforços (Êxodo 22) e riscos (Eclesiastes 9:11-18).

[14] *Slippage*: https://bit.ly/3qS0bzC

[15] Ciclos civilizacionais: https://bit.ly/3wdzxSz

[16] Quem é John Galt?: https://bit.ly/3z8dnE2

[17] Medidas de dominância derivadas de *market cap* como o disponível no coinmarketcap.com não valem nada. Primeiro, que são listados centenas de ativos que não são *use tokens* (criptomoedas de uso) — lá são listados *equity tokens* (equivalente a uma ação) ou *stable coins* (*IOUs* colateralizados, em tese) e até mesmo *stable* bitcoins em outras plataformas; segundo,

que a maioria das *shitcoins* listadas tem valores e volumes descaradamente manipulados, sem qualquer quantidade relevante de volume em ordens.

[18] *Why BTC is the honey badger of money*: https://bit.ly/362H1NO (arquivado: http://archive.today/JOcCd).

[19] Se ciência não é mais método e sim consenso de comunidade, quando a comunidade está corrompida por concursos e seleções fraudadas e por distorções derivadas de financiamento governamental, então seu consenso não vale nada. Semmelweis, o primeiro a afirmar que lavar as mãos reduzia infecções, foi considerado louco e morreu no hospício, mesmo com demonstração empírica e publicações dentro dos padrões da época.

[20] A guilhotina de Hume cai na guilhotina: https://bit.ly/3ApvZjr

[21] Internado em hospício involuntariamente e morto no processo (Ignaz Philipp Semmelweis), resultou no *Semmelweis Effect* na psicologia comportamental: https://bit.ly/354nMmp (arquivado: https://archive.vn/3SeiS).

[22] Kelsen foi refutado por Voegelin (e, após isso, pela realidade e Lógica Argumentativa) - O dilema da Justiça natural: https://bit.ly/3dsiO7P (arquivado: http://archive.today/ORgoX).

[23] *Thank God for Bitcoin:* https://amzn.to/3xaQUog

[24] *Bitcoin: The Most Islamic Form of Money?* https://spoti.fi/3pE1BNe

[25] El Salvador tem primeiro presidente com *laser eyes:* https://bit.ly/3x7c5ra

[26] Como Saylor se refere aos *bitcoiners*: "Bitcoin é um enxame de vespas cibernéticas servindo a deusa da sabedoria, alimentando-se o fogo de verdade, exponencialmente cada vez mais inteligente, mais rápido e mais forte atrás de uma parede de energia criptografado" https://bit.ly/3xfYdvd *(twitter)*

[27] Thread Mises Capital vs Samy Dana: https://bit.ly/3ys87JQ / Com Bitcoin ultrapassando os R$ 233 mil, Samy Dana perderia hoje aposta contra Mises Capital (8 de fevereiro de 2021): https://bit.ly/3jpjwpA

[28] *Men Going Their Own Way:* https://bit.ly/3qLbdq9

[29] Bitcoin: https://en.wikipedia.org/wiki/Bitcoin

[30] *Wiki Bitcoin*: https://en.bitcoin.it/wiki/Main_Page

[31] *Bitcoin Revolution*: https://amzn.to/3v2oBXy

[32] IMB: https://www.mises.org.br/Ebooks.aspx?type=99

[33] Rothbard Brasil: https://rothbardbrasil.com/biblioteca/

[34] Inflação, base monetária e agregados: https://bit.ly/2Twp5Zf

[35] Os recentes eventos deixaram ainda mais claro: dinheiro de verdade é o ouro e você empobreceu: https://bit.ly/3532Yvs

[36] Quantidade de moeda criada – base monetária: https://archive.vn/dDRkU. Agregados monetários (quantidade de reais) triplicaram na década com queda de PIB real. Desde o início do Plano Real até 2019, *broad money* aumentou mais de 42x, entretanto, o Real só perdeu 97% do seu valor em ouro, originalmente R$11.5 o grama e hoje R$340,00 graças ao aumento de estoque de riqueza, que caiu na última década. Nesse caso, usamos os dados de "*broad money*" do Banco Mundial (M3 ou M4), "*narrow money*" seriam os M1 e M2. Para dados detalhados, vide relatórios do Banco Central na referência seguinte.

[37] 50% mais reais em 2020: https://bit.ly/351Oufs (arquivado: https://archive.ph/s8uP9)

[38] Estatísticas monetárias e de crédito do BCB: https://archive.ph/p3p6j

[39] Como governo gosta e precisa de inflação: https://bit.ly/3Be30ih

[40] *Whitepaper*: https://bitcoin.org/en/bitcoin-paper

[41] A mensagem é uma manchete do jornal britânico *The Times* de 3 de janeiro de 2009: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks* (*The Times 03/Jan/2009 "Chanceler à beira do segundo resgate aos bancos"*, tradução livre).

[42] *Satoshis' posts*: https://bit.ly/3g889k9

[43] *FRED data*: https://fred.stlouisfed.org/series/FYFSD

[44] "Curso forçado" consiste no dever legal de aceitar a moeda fiduciária estatal para qualquer pagamento, "*legal tender*", como escrito hoje nas cédulas onde havia "conversível por ouro".

[45] Base monetária global era de 94,8 trilhão de dólares em 2020 *(Only One Number Mattered to Global Markets in 2020):* https://archive.ph/6q8I3 em tempo real; *Fiat Market Cap:* https://fiatmarketcap.com/

[46] Alodial é sem vínculos ou ônus, como cédulas e contrário a saldo em banco.

[47] *An Escalating War on Cash*: https://bit.ly/3gkIoMs (arquivado: http://archive.today/7VOtg).

[48] Nota de 500 euros - Obs.: *Pararam de emitir essa nota, mas ainda é válida e circula.

[49] *Gold Reserve Act*: https://bit.ly/3hh2bhm

[50] "Qual o melhor investimento da década? Ouro lidera; Bolsa perde da inflação": https://archive.vn/3CGCR

[51] *Capital asset pricing model*: https://bit.ly/3whO13Q e VPL: https://bit.ly/3jFEam3

[52] Teoria da Captura Regulatória: https://pt.wikipedia.org/wiki/Captura_do_regulador

[53] Quarentena e Lockdown foram crimes contra a humanidade: https://bit.ly/2SQHcsE (arquivado: http://archive.today/Qf26W).

[54] *Main Street bailout failed:* https://bit.ly/2Ugd8qB

[55] Arthur C. Clark previu em 1964 a obsolescência das cidades em decorrência da viabilidade futura de comércio e serviços remotos: *Arthur C Clarke predicting the future in 1964-Trimmed.flv*: https://bit.ly/3yfPyZj

[56] Nascimentos em 2020 caem 5,66%: https://bit.ly/3zjsQ43 (Arquivado: http://archive.today/cMsl7)

[57] *Fertility rate:* https://data.worldbank.org/indicator/SP.DYN.TFRT.IN?locations=BR e uma análise aprofundada por Peter Zeihan: https://www.youtube.com/watch?v=EeGX105X7ac

[58] Conceito claro na "autorresponsabilidade" da filosofia objetivista: https://archive.vn/isrO1

[59] Diversos artigos indicam que até 60% dos homens entre 20-35 anos em países de primeiro mundo apresentam tendências "herbívoras" em decorrência das mudanças de papéis e valores sociais – perdem interesse em sexo, alimentação ou realizações materiais relacionadas a valores masculinos, identificados no "Código dos Homens" (Jack Donovan) (https://bit.ly/3xgOaWN) em força, coragem, destreza e honra: https://bit.ly/3qOz4VV – representando um risco à "armadilha malthusiana", situação de colapso civilizacional devido à estagnação tecnológica.

[60] Para entender que a maior parte do gasto de inteligência soviético era contra inteligência (subversão e desmoralização) vide Heitor de Paola, no *Eixo do Mal Latino-Americano e a Nova Ordem Mundial ou* Yuri Bezmenov https://bit.ly/3hvV1EX

[61] Para entender como a "pirâmide nutricional" recomendada pelo governo é parte da engenharia social ler "*The Fiat Standard*" do Saifedean ou: *What made the Ancient Egyptians Fat and Sick?* https://bit.ly/3BgBUa7

[62] Porque oligarcas bilionários são esquerdistas: https://bit.ly/3AcHryZ (arquivado: http://archive.today/s25br).

[63] Paralaxe Cognitiva: https://bit.ly/3wcXNEt (arquivado: http://archive.today/TNtxU).

[64] Demonstrando o conceito de religião política e o fato de que nunca houve real separação de religião e Estado e sim substituição da Igreja pela religião política (ou religião civil de Rousseau): https://archive.vn/HVwXE A voz do povo é a voz do diabo, a voz de Deus é a LEI natural e bíblica, Deus é a verdade (João 14:6) e tudo que não presta (ódio, inveja, vícios, crime, comunismo…) vem da mentira (João 8:44).

[65] *Idiocracy* (como motivações distorcidas podem levar a idiotização mundial): https://bit.ly/2XOF1I0

[66] *Paypal* bloqueia conta de Olavo de Carvalho por disseminação de *fake news*: https://bit.ly/3hArDNQ (arquivado: https://archive.vn/EkzAu).

[67] Hayek - Arrogância Fatal: https://bit.ly/2V4k5LU e o Uso do Conhecimento na Sociedade: https://bit.ly/3ykqfpn

[68] Expressão em inglês equivalente a "ter o seu c* na reta".

[69] Termo referido em clássicos como *Pense e Enriqueça*, de Napoleon Hill, e *Pai Rico*, *Pai Pobre*. Livros mais adequados para o contexto atual com o mesmo fito seriam *12 regras para a vida*, de Jordan Peterson, e *Rational Male*, de Rollo Tomassi.

[70] Dinheiro *versus* Moeda - *Hidden Secrets Of Money* Ep 1 - Mike Maloney https://bit.ly/3dIuvqT

[71] A evolução dos meios de troca no Novo Mundo ocorreu mais rápido que no Velho Mundo, mas na mesma ordem, demonstrando que é um processo natural.

[72] Bitcoin é a próxima etapa lógica na tecnologia do dinheiro: PlanB @100trillionUSD (Twitter).

[73] *The Problem of Social Cost*: https://bit.ly/3AqNmR1

[74] *Property rules, liability rules, And inalienability: one view of the cathedral*. *Harvard Law Review*, *1972:* https://archive.vn/yh2bo

[75] Mais uma prova do "Neo Feudalismo" de Max Keiser e da infância mental é o documentário "Alquimia da Verdade", no qual um empresário é obliterado moral e financeiramente por perseguição estatal e ainda acha que vai encontrar restituição na (in)justiça estatal: https://bit.ly/3ApJ6Bl

[76] "*it is more or less impossible to reach Bitcoin maximalism while retaining any amount of trust in the system"*- Why The Yuppie Elite Dismiss Bitcoin: https://bit.ly/3h3BbSp (arquivado: http://archive.today/qUl1C) ou Por que os Faria Limers rejeitam o Bitcoin? https://bit.ly/3qHtRPJ (arquivado: http://archive.today/ktfJm).

[77] Ross Stevens, da NYDIG, explicando como gente com alto QI deixa de entender o BTC por falhas cognitivas de viés (em regra por acreditar em instituições falidas por terem funcionado no passado): *Ross Stevens - MacroMinds | NYDIG - The Beauty of Bitcoin:* https://bit.ly/3yfRIIp

[78] Quarto mês de pânico: onde estão as evidências? https://bit.ly/3yaHN7d (arquivado: https://archive.vn/qGF2b).

[79] Não há "ciência estabelecida" que corrobore o uso de máscaras: https://bit.ly/2TilrSw (arquivado: https://archive.vn/D41Ut).

[80] *Cumulative number of coronavirus-positive (COVID-19) Cumulative number of coronavirus-positive (COVID-19) patients confirmed on Diamond Princess cruise ship docked in Japan as of April 16, 2020:* https://bit.ly/3he8hze

[81] *USS Theodore Roosevelt, COVID-19, and Ships: Lessons Learned: https://bit.ly/3hgG0rM (arquivado: http://archive.today/xflNN).*

[82] Evolução da Programação Web: https://bit.ly/3jHLRrU

[83] Engenheiro do google confessando manipulação das buscas nas Eleições de 2020, Vídeo produzido por *Project Veritas*: https://bit.ly/3qOkbTM

[84] Dilma se encontra com Zuckerbeg no Panamá: https://glo.bo/3dsT22Z (arquivado: http://archive.today/coVe4).

[85] China tem um plano para dominar a Internet do mundo todo: https://bit.ly/36dmPss

[86] Hitler tentando salvar o mundo, com conceitos socialistas totalmente errados: https://youtu.be/PQGMjDQ-TJ8

[87] O caminho da servidão: http://rothbardbrasil.com/wp-content/uploads/arquivos/caminhodaservidao.pdf

[88] ISTOÉ afirma que presidente "além de broxa deve ser gay passivo": https://bit.ly/3AnDkQF (arquivado: http://archive.today/xkbk2).

[89] Desnazificação é o processo de destruição (financeira, moral e política) das elites criminosas no final de regimes de exceção. Nos países comunistas que as elites burocratas não foram condenadas e punidas por seus crimes – como a Rússia, Ucrânia, Moçambique e Angola – as famílias desses burocratas continuaram sendo os donos dos países e mantendo suas vítimas em regimes de miséria e repressão. Compare os vizinhos Bielorrússia com Lituânia ou Letônia com triplo do PIB *per capita* e verá a diferença: *Why is UKRAINE the POOREST country in EUROPE? - VisualPolitik EN:* https://bit.ly/3mNrH1h

[90] Larápios do Covidão: https://bit.ly/3wkmkaB (arquivado: http://archive.today/M4SGw).

[91] Brasil tem anos seguidos de queda no consumo de energia: https://bit.ly/2UU6Xsv (arquivado: http://archive.today/Z11GP).

[92] Fuga de cérebros sem precedentes, demonstrando que com Bolsonaro a dominância oportunista foi ampliada: https://bit.ly/3xhMEU7 (arquivado: http://archive.today/bSmiH).

[93] José Dirceu: https://bit.ly/3jrtE1u (arquivado: http://archive.today/0A9zZ).

[94] Moro determinou prisão em sala de Estado Maior, com luxos sem precedentes nem previsão legal para Luiz Inácio: https://glo.bo/3heZcVE (arquivado: http://archive.today/3gagZ).

[95] Se o regulamento do SINARM acabou com critério subjetivo para autorização de compra de armas, ele adicionou mais de uma dezena de dispositivos desarmamentistas, como a proibição automática a depender dos índices de criminalidade na região, só os muito ricos podem ter arma no governo Bolsonaro, exatamente porque os seus indicados para o setor eram militantes progressistas: https://bit.ly/361uhXD (arquivado: http://archive.today/VLDnF).

[96] 14 leis feministas de Bolsonaro em menos de 2 anos: https://bit.ly/2SIbLRe (arquivado: http://archive.today/wdcn2) e a 15# foi a Lei 14.188 que institui crime com tipo aberto de "violência psicológica".

[97] Página da redação vazada, gráfica sem licitação, confusão no gabarito e erros em notas – sem contar conteúdo progressista militante: https://archive.vn/vzuyc considerado o mais vergonhoso internacionalmente: https://archive.vn/79XXR

[98] Bolsonaro se submete a ditadura comunista mais assassina da História: https://bit.ly/2UOHCQJ (arquivado: http://archive.today/GpLvX).

[99] Armadilha da dependência: https://bit.ly/3AeOK9h arquivado: http://archive.today/sjvWw

[100] 66 milhões: https://glo.bo/3x9oI5x arquivado: http://archive.today/o1hDI

[101] *The complicated truth about China's social credit system* https://bit.ly/3jhY31J (arquivado: http://archive.today/GsiAl)

[102] *Organ harvesting* ("doações involuntárias" de órgãos de dissidentes): *How to Make Money in China: Selling People's Organs:* https://bit.ly/3hfhXJH

[103] A patente do número Pi: https://bit.ly/3dDXEU0

[104] Há muito material no *YouTube* deles – embora muitas coisas que defendem sobre o *legacy* (sistema convencional) e seus envolvimentos com empresas com baixa admiração na comunidade (XDEX/Atlas) sejam polêmicas, sendo acusados de serem Faria Limers.

[105] Roteiro de estudos com link para recursos: https://bit.ly/3w8Ixt9

[106] Estado é escravidão? Paulo Kogos: https://bit.ly/3vcOILo

[107] KoreacomK: https://twitter.com/KoreaComK

[108] Fontes em inglês devem incluir: @PeterLBrandt @alessiorastani @tonevays @chrisdunntv, BlackpillBr (https://t.me/bitcoinblackpill_BR) e Raicher (https://t.me/nostreidamos)

[109] Introdução indefectível: https://bitcoinheiros.com/intro-bitcoin/

[110] Futuro descentralizado: https://bit.ly/3v8HyYL

[111] Redes de confiança formais e informais: https://bit.ly/3iwirwi

[112] Uma rede de confiança *(WoT – web of trust)* é um grafo que estabelece uma relação de confiança entre duas partes, mesmo que elas não se conheçam previamente, através de ligações diretas ou indiretas: https://bit.ly/3h52vzN (Arquivado: https://archive.vn/dgHRu) .

[113] MOOC grátis da Universidade de Nicosia: https://www.unic.ac.cy/blockchain/free-mooc/

[114] *Data-Secrecy Export Case Dropped by U.S.Jan. (12, 1996):* https://nyti.ms/2UOKWeF (arquivado: https://archive.vn/GSjk0) / O criador do PGP: https://bit.ly/3hb25bb / https://pt.wikipedia.org/wiki/Phil_Zimmermann

[115] Asimov sobre 2020 e *digital divide*: https://www.youtube.com/watch?v=-_4xkkIKW2c muitos futurólogos estudam cenários de "economia da abundância" (Kurzweil) ou "sociedades pós escassez" (Isaac Arthur): https://www.youtube.com/watch?v=_Kt7883oTd0

[116] *The Saylor Series*: https://bit.ly/2SMmutV

[117] Vide *FAANGs* - Facebook (FB), Amazon (AMZN), Apple (AAPL), Netflix (NFLX), and Alphabet (GOOG) *versus* S&P500.

[118] Uma interpretação particular da hierarquia das necessidades particulares em homens e mulheres, sob uma perspectiva *MGTOW*: https://bit.ly/2SK2yHV

[119] 12 camadas da personalidade: https://bit.ly/3qDKXhC

[120] *Rankings* de QI do Wikipédia e exames do Pisa.

[121] *Open borders IQ and civilization:* https://bit.ly/3jFVFCD

[122] Se pretende ter filhos, entenda o "teste do *marshmallow*" para entender como a baixa preferência temporal é mais determinante para o sucesso que QI. Mais importante ainda que autocontrole é planejamento para evitar as tentações (sem arriscar *esgotamento do ego)*: https://bit.ly/3wpzGCR

[123] *IQ and national success:* https://bit.ly/2UolWuI

[124] Como descrito por Lobaczewski na "Ponerologia Política", a patocracia é o sistema em que "todas as posições de liderança devem ser preenchidas por indivíduos com anomalias psicológicas" e que "seu nível intelectual ou habilidades profissionais não devem ser levados em consideração" e que sua consequência é "Sob tais condições, nem uma área da vida social pode se desenvolver normalmente, seja na economia, cultura, ciência, tecnologia ou administração. A patocracia progressivamente paralisa tudo". Outra obra importante sobre o tema é *Mentalidade Esquerdista*, de Lyle Rossiter.

[125] Vide "*Shadow World"* de Robert Chandler e os clássicos "*1964, O Elo Perdido"*, de Vladimir Petrilak, e "*Desinformação*, de Ion Pacepa: Sobre as ações atuais de captura de elites e dirigentes políticos pela China, é recomendável assistir: https://bit.ly/3wfSpAz

[126] Foro de São Paulo e "Teologia da Libertação": https://bit.ly/3wkkqa6 para detalhes do acordo de 2019 entre Vaticano e Pequim para entregar cristãos para expurgos e garantir cardeais nomeados pelo partido comunista no próximo conclave vide Cardeal Zen: https://bit.ly/3Aoyym3 (o Papa argentino ser um agente infiltrado, explicaria o silêncio e colaboração da Santa sé dos crimes da ditadura mais assassina da História, promovendo genocídios em lugares diversos como Xinjiang, Mongólia Interior e Tibete). Até militantes de esquerda denominam o "acordo secreto" como "completo controle do PCC" (mencionando que as imagens de Jesus em igrejas tinham sido substituídas pelas de Mao, assim como a "Bíblia oficial" rescrita) e que seria em troca de US$2Bi/ano: https://bit.ly/3hbbOhM

[127] Indicador com 95% de sucesso em um ano, fazer o contrário do que recomenda a CNBC: https://bit.ly/3jHcBZi

[128] Curva de Rahn: https://en.wikipedia.org/wiki/Rahn_curve / Gasto público máximo para a curva de Rahn é entre 15-25% do PIB e curva de Laffer na Califórnia: https://bit.ly/3jHBd4v (arquivado: https://archive.vn/3dCvE).

[129] Efeminação dos valores, hedonismo, redução da fecundidade, diluição da moeda com aumento do assistencialismo são elementos comuns no colapso de diversas civilizações: https://bit.ly/3ABCJLs

[130] @Thaitata https://twitter.com/thaitata/status/1054576337351008256

[131] *The Red Pill (*documentário*)*: https://bit.ly/3jFfGJv

[132] Como funcionou a escravidão e os esquemas de promiscuidade obrigatória: https://www.youtube.com/watch?v=zkcVkmzeJ4U. e https://www.youtube.com/watch?v=_AS-5kceQ_A.

[133] *Iron Rules*: https://bit.ly/36bfh9H

[134] Stefan Molyneux: https://bit.ly/2RpKgLv

[135] *Welfare* destruindo fecundidade: https://bit.ly/3jBVSXv

[136] Hipergamia e poliginia são fatos etnobiológicos e não culturais e não são ignoradas pelas leis de família feministas que inviabilizam famílias, elas são usadas para destruir famílias, o exemplo ápice disso são os herbívoros (*herbs*) japoneses (pessoas jovens que desistem de buscar sexo ou relacionamentos): https://pt.wikipedia.org/wiki/Herbs e as mulheres pagando alto para ser inseminadas por desconhecidos: https://bit.ly/3yleKOx

[137] Porque homens não querem mais casar: https://bit.ly/3ylIP0p

[138] Mulher decide se vai ter sexo, homem se vai ter compromisso: https://bit.ly/3yl8WE8 (arquivado: http://archive.today/YthEH)

[139] Como explica o brocardo "uma chave que abre qualquer porta é uma chave mestra e a porta que se abre com qualquer chave uma arrombada", devido ao dimorfismo, mulher pode enganar homens sobre paternidade, mas o contrário não é possível: *Mater semper certa est*

[140] União com mulher alheia, mesmo repudiada sem culpa, é adultério e amaldiçoa por gerações: Mt19:9 "Eu vos digo, porém, que qualquer que repudiar sua mulher, não sendo por causa de prostituição, e casar com outra, comete adultério; e o que casar com a repudiada *também* comete adultério". Por isso se diz que as "mães solteiras" devem permanecer "solteiras" (se o casamento é o sexo, só existe mulher solteira se inseminada virgem) - e encerrando as leis feministas e de paternidade involuntária a maioria delas também deixariam de ser mães. A mulher, em muitos sistemas jurídicos pode escolher: 1) se fica fértil ou não; 2) se é coberta ou não; 3) se inseminada permite ou não nidação; 3) se mantém gravidez ou aborta; e, se parir, 4) se dá criança ou registra em seu nome - e o homem tem paternidade forçada apenas por DNA, quando não imposta até sem DNA, como nas teratologias de multiparentalidade e "paternidade afetiva involuntária".

[141] Dessa assimetria de poder entre homens e mulheres que resulta a explosão de filhos fora do casamento, mais vulneráveis ao crime, pobreza e submissão e com menos chances de desenvolvimento. Vide Stefan Molyneux, *The Truth About Single Moms:* http://www.fdrurl.com/single-moms-transcript (*The Truth About Single Moms*: https://bit.ly/3xbjINH)

[142] Gênesis 1:28 "Deus os abençoou: [Frutificai – disse ele – e multiplicai-vos, enchei a terra e submetei-a. Dominai sobre os peixes do mar, sobre as aves do céu e sobre todos os animais

que se arrastam sobre a terra]” demonstrando que a militância por "direitos dos animais" é demoníaca.

[143] Na França, há mais de 15 anos, é crime fazer DNA privado de seu filho para saber se é seu, no Brasil também já houve caso de justiça determinar paternidade involuntária diversas vezes (expressamente por motivo patrimonial, como no caso do goleiro Bruno): https://bit.ly/3dw6N0Z (arquivado: http://archive.today/YSglY).

[144] Por não compreenderem quais critérios os machos as avaliam, mulher por vezes se avalia segundo critério de valor para homens. Os homens são avaliados pela capacidade de prover segurança e as mulheres pela fertilidade e fidelidade que podem oferecer - e não por renda, independência ou formação acadêmica.

[145] “Filhotes não são bebês e [mãe de pet] não são mães”: https://bit.ly/3ApQU5Y sociedades que adoram animais, usualmente, sacrificam humanos inocentes. Direitos animais como subversão moral: https://bit.ly/368Fq9j

[146] Para entender comportamentos evolutivos ler o seminal “O Macaco Nu” de Desmond Morris, “O Gene Egoísta” de Dawkins ou *Tribalism and the fall of West:* https://bit.ly/3hz9n7K

[147] Princípio da não agressão (Daniel Fraga): https://bit.ly/3qKDQnh (Visão Libertária): https://bit.ly/3dGpdMt

[148] Geração Paulo Freire: exposição o “Cu é Lindo” na UFBA explica o resultado no Pisa. O que os universitários fazem hoje explica o resultado negativo do Brasil no Pisa, fruto de uma geração ideologicamente manipulada: https://bit.ly/36cqKG0 (arquivado: http://archive.today/cnIyq).

[149] Como o Estado destrói a família: https://bit.ly/3hiCFHz (arquivado: https://archive.vn/w1AXM).

[150] Escurecimento global: https://bit.ly/3AsyEJt

[151] Planeta Azul em Algemas Verdes: O que está em perigo: o clima ou a nossa liberdade?: https://amzn.to/3jGgcH6

[152] “O Estado não Conserva a Biodiversidade": https://bit.ly/3jBWwEp

[153] Desastre de Kyshtym: https://bit.ly/2SLIZiB

[154] Estimativas variam que entre 10 e 28 milhões de mortos de fome devido à matança dos pássaros na Campanha das Quatro Pragas: https://bit.ly/2UkEn3s

[155] Ambientalista Libertário: https://bit.ly/3Ddu1Ei

[156] *Gell-Mann amnesia effect: https://bit.ly/3wfzUMD*

[157] Os direitos naturais e lógicos derivam da liberdade (ou autopropriedade para Hoppe) como fato, inclusive de adquirir, de maneira originária ou derivada, outros direitos. Consentimento é legitimação e a diferença entre estupro e sexo e entre doação e furto. Direitos públicos negativos são aqueles que limitam ações do governo e direitos públicos positivos (de receber algo, como direito a educação e saúde) não podem ser prestados sem violar PNA, não sendo então legítimos.

[158] Convergência de *bitcoiners* (como Saifedean), Jordan Peterson e sua família e o médico recordista Shawn Baker a dietas carnívoras: *Carnivore Diet: Why would it work? What about Nutrients and Fiber?* https://bit.ly/3jGv4FG

[159] Pecuária salva o mundo. *Are Cows really Bad for the Planet?* https://bit.ly/3wfzWnJ

[160] *Democracy or Republic?* https://bit.ly/3hdGIpC (arquivado: http://archive.today/zD9SA). diversas frases indefectíveis dos pais fundadores em repúdio a democracia como *"Democracy is two wolves and a lamb voting on what to have for lunch. Liberty is a well-armed lamb contesting the*

vote!” Benjamin Franklin ou *“Remember, democracy never lasts long. It soon wastes, exhausts, and murders itself*” John Adams ou "*A democracy is nothing more than mob rule, where fifty-one percent of the people may take away the rights of the other forty-nine”* Thomas Jefferson.

[161] A relação conturbada entre os maximalistas e o obeso que recomenda jejum é detalhada em: https://bit.ly/2ThyYKm (arquivado: http://archive.today/uqEUE).

[162] Uma nova abordagem para os problemas de desenvolvimento: https://bit.ly/3dydrnp (arquivado: http://archive.today/BkIOb).

[163] *The Bitcoin Standard*, como *As seis lições*, também correlaciona o colapso de civilizações e nações com a diluição de valor de suas moedas, decorrente de *déficit* público: https://bit.ly/3x9Ou9K

[164] *Your nation's IQ matters*: https://bit.ly/3hwxmo2

[165] Assim, aquelas pessoas que tenham uma baixa preferência temporal, estarão dispostas a renunciar a bens presentes em troca de conseguir bens futuros com um valor não muito maior, e efetuarão trocas entregando seus bens presentes a outros que tenham uma preferência temporal mais alta, e portanto, valorizem com mais intensidade relativa o presente do que o futuro…

Democracia e empobrecimento segundo Hans-Hermann Hoppe: https://bit.ly/3ymEtGe / (arquivado: http://archive.today/DFdAP).

Preferência temporal: https://bit.ly/2SMHMaP

[166] Embrapa: https://www.cnpm.embrapa.br/projetos/gite/

[167] Geração Nem-Nem+: uma bomba-relógio: https://bit.ly/2UgwrjH (arquivado: https://archive.vn/2ISHt).

[168] Mateus 20:1-16: Parábola dos Trabalhadores das Vinhas

[169] *Should We End the Fed?* https://bit.ly/2TpNm3j

[170] Murray Rothbard em *Manifesto Libertário*. Um panorama atualizado é dado pelo *bitcoiner* Max Keiser em seu Keiser Report (da russa RT), informando com dados oficiais como: 1) a maioria dos universitários não aumentam sua capacidade mental no curso (e muitos até perdem inteligência e habilidades); 2) como há mais que o dobro de formandos que demanda por formados, resultando em 3) na maioria dos graduados executando profissões que não demandam formação, tendo na universidade investimento perdido, com altíssimo custo de oportunidade: https://bit.ly/3jFh1jr

[171] Lei de Ferro da Oligarquia: https://bit.ly/38dwNv0

[172] Como bem lembrado na Revolta de Atlas “basta criar leis que não podem ser cumpridas e faturar em cima dos culpados”. Por que existem tantas leis no Brasil: https://bit.ly/3srAjLr

[173] *Curley Effect*: https://bit.ly/3AnMQTT

[174] Estados totalitários como a Coreia do Norte ou Cuba (que proíbem ou restringem o acesso de seus escravos/cidadãos à Internet) podem continuar existindo após o fim dos Estados Sociais – até que os mercados de apostas de morte sejam totalmente desenvolvidos e a caridade financie a eliminação dessas ditaduras. Plataformas de apostas descentralizadas de morte já eram concebidas e formalizadas em 2004 como consequência de *criptos* alodiais, antes mesmo do conceito de *smart contracts: Assassination Politics (by Jim Bell)* https://cryptome.org/ap.htm *(arquivado: http://archive.today/nnPBI)*

[175] *Fork* é divisão de sistemas.

[176] Versão em português: https://bit.ly/3yo0zIm (arquivado: https://archive.vn/meIQi).

[177] Who is Satoshi? https://bit.ly/3gAqeai

[178] Tim May, *The Crypto Anarchist Manifesto*: https://bit.ly/2Tmpcqd (arquivado: https://archive.vn/7VfHH).

[179] Por que Satoshi se ausentou e como: https://bit.ly/3hlHPT1 (arquivado: http://archive.today/Sn6Hv).

[180] Executando um *full node*: https://bit.ly/3ycXP0K (arquivado: https://archive.vn/0Brfe).

[181] Distribuição global de nós do Bitcoin: https://bitnodes.io (arquivado: https://archive.vn/8RsZq).

[182] Ainda é possível rodar nó pelo TOR sem expor seu IP: https://bit.ly/3x4N8No

[183] A fabulosa ilha Bitcoin: https://bit.ly/3qBfLzr (arquivado: https://archive.vn/pvaOx).

[184] Exemplo é a transmissão de bitcoins por rádio, triangulada pela Lua, entre Márcio Gandra, Rafael Silveira, Narcélio Filho, André Alvarenga e Paulo Jr.: https://bit.ly/3hp1Bxa (arquivado: http://archive.today/CSFkJ).

[185] "Descentralizado" significa que o Bitcoin não tem autoridade ou estrutura central nem é democrático, é composto por atores independentes e a rede só decide mudanças por consenso. Caso um grupo discorde de modificação, pode continuar na versão anterior (*fork*). A rede é distribuída e descentralizada para ser antifrágil, a destruição de uma parte dos mineradores ou nós não é capaz de pará-la, todos os milhares de nós e mineradores teriam que ser destruídos simultaneamente para destruir o Bitcoin.

[186] *Money Over Internet Protocol:* imagem da Pantera Capital

[187] Bitcoin: um sistema de dinheiro eletrônico ponto a ponto: https://bitcoin.org/en/bitcoin-paper (arquivado: https://archive.vn/KmpTS)

[188] Primeiras reportagens sobre BTC em mídias convencionais foram em 2011, como essa da Globo: https://glo.bo/3qEE1jW (arquivado: http://archive.today/HLtQK). ou https://tcrn.ch/3jx9EdJ (arquivado: http://archive.today/cjofd).

[189] *Dez formas de explicar Bitcoin*: https://bit.ly/3dvZaYk (arquivado: https://archive.vn/A6WBg).

[190] *Guerra ao dinheiro*: https://bit.ly/2Tnp8Xg (arquivado: https://archive.vn/GkfEJ).

[191] Ninguém tem o poder de confiscar ou alterar transações que já aconteceram. Todas as informações estão replicadas em milhares de nós em consenso. Onde é criminalizado, pode continuar sendo transacionado com auxílio da rede TOR, VPN, com acesso físico à Internet de outra jurisdição por satélite ou qualquer meio de comunicação, como SMS, carta ou chamada discada; e, normalmente, passa a valer mais como na Venezuela: https://bbc.in/2SHUZlc (arquivado: http://archive.today/TAz26). O *spread* (ágio) no preço do bitcoin normalmente expressa custo de transação marginal derivado do controle de capitais do país.

[192] *Satoshi's quotes Re: Bitcoin does NOT violate Mises' Regression Theorem*: https://bit.ly/3AdNza5 (arquivado: http://archive.today/UtxnY).

[193] Vide: https://coinexplorer.sk/co-je-btcoin

[194] *Bitcoin Is Not Too Volatile*: https://bit.ly/2UWdROl

[195] BTC na Venezuela: https://bit.ly/2UitG11 (arquivado: https://archive.vn/S69oj).

[196] Esposa de Rocelo: https://bit.ly/3qAWQ7G (arquivado: https://archive.vn/H448F).

[197] MBL e lavagem de dinheiro: https://bit.ly/3xaDYPl (arquivado: https://archive.vn/f3HDz).

[198] Pichardo: https://bit.ly/3ymi4Ja (arquivado: https://archive.vn/W7yam).

[199] *Bitcoin as a new asset class* https://bit.ly/3Af3t4a (arquivado: https://archive.vn/NqRZL).

[200] *WTF happened in* 1971? https://wtfhappenedin1971.com/ muitos exemplos históricos são demonstrados de maneira detalhada por Mike Maloney no *Hidden Secrets of Money* e nas *Seis Lições*.

[201] *Bitcoin Revolution*: https://amzn.to/3qIzcGD

[202] *The Bitcoin Reformation - Podcast (Bitcoin Audible): The Bitcoin Reformation - by Tuur Demeester*: https://bit.ly/3jqIohc

[203] *Bitcoin and the poor*: https://bit.ly/3jxtcPk (arquivado: http://archive.today/KHr80).

[204] Mateus 5:17-19

[205] *Quantum computing and Bitcoin:* https://bit.ly/3jwp6Hi (arquivado: https://archive.vn/SBdrL).

[206] *Cryptology ePrint Archive:* https://bit.ly/3qRrcmD (arquivado: https://archive.vn/sFOam).

[207] *Is Quantum Computing a Threat to Standard Cryptocurrencies?* https://bit.ly/3qHi9Vd (arquivado: https://archive.vn/hvN29).

[208] *ENCRYPT II*: https://www.ecrypt.eu.org/.

[209] No século XIX, era comum entre trabalhadores das minas de carvão a prática de monitorar o nível de gases tóxicos usando **canários**. Esses eram primeiros a morrer, sinalizando o momento em que os mineiros deveriam deixar a mina.

[210] *Bitcoin and me*: https://bit.ly/366amqK (arquivado: http://archive.today/skZlp).

[211] Quase R$ 120 bilhões em bitcoin estão perdidos para sempre, estima empresa: https://bit.ly/3y2oCN4 (arquivado: https://archive.vn/PVDp2).

[212] É palavra adicional às 12, 18 ou 24 palavras do mnemônico (seed phrase) da carteira. Cada mnemônico pode conter inúmeras *passphrases*, formando carteiras únicas e independentes.

[213] *Dead man switch* na *Lightning Network:* https://bit.ly/2SEmpZb (arquivado: http://archive.today/QkcBm). / https://github.com/joostjager/deadmensbutton/ / https://github.com/joostjager/whatsat/tree/whatsat-paid

[214] Isso sem adiantar todos os aspectos específicos de *valuation* de criptos explicados no ponto *por que Bitcoin é o Rei?*

[215] *Gold Silver Ratio:* https://bit.ly/36428PL (arquivado: https://archive.vn/Pkbhk).

[216] *Por que Ethereum é golpe:* https://bit.ly/3w6Z6EX (arquivado: http://archive.today/5oWbA).

[217] Pré-mine do ether perpetua controle dos criadores que não colocaram 1 satoshi no projeto: https://bit.ly/3yc34Oc (arquivado: http://archive.today/7QYsl). Todos os ethers até hoje minerados não superam o pré-mine distribuído para fundadores bilionários que escolhem quais transações são válidas e anulam outras.

[218] Pesquisar sobre os casos, no Brasil, de Renné Sena e Antônio Domingo.

[219] "Ação meme" sobe 1400% em um dia:: https://bit.ly/3js9rc1 (arquivado: http://archive.today/tEBXm).

[220] *Cash and Carry:* https://bit.ly/3h5zMuQ (arquivado: http://archive.today/01Mjy).

[221] *Lending* passo-a-passo - Como receber juros usando o *Funding* da Bitfinex: https://bit.ly/2TrAF7M

[222] Atualmente, existem empresas como a *Blockfi*, que pagam 5% a.a. em *stable* de ouro, porém, o investidor incauto sofre triplo risco de custódia, perdendo tudo em caso de falha da *Blockfi* ou da *blockchain* cuja *stable* está registrada ou do emissor.

[223] Pense e enriqueça: https://bit.ly/3qIAEc3

[224] Anarquia em Pessoa: https://bit.ly/2SD5g1U (arquivado: http://archive.today/ayddq).

[225] *Social credit systems*: https://en.wikipedia.org/wiki/Social_Credit_System.

[226] A eliminação de dissidentes é uma constante em fraudes concursos e processos (assassinatos de reputação) em países bolivarianos como Venezuela e Brasil, mas começou prática pública nos EUA: Biden Administration Asks Americans to Report 'Potentially' Radicalized Friends and Family: https://bit.ly/3AgCkhe (arquivado: http://archive.today/msnjh) a ponto de dissidente da "Coreia da Morte afirmar que o ambiente acadêmico americano com sua "política de cancelamento" é tão patológico quanto a RPCD: Even North Korea is not this nuts': Defector after graduating from American university: https://bit.ly/3Air8AP (arquivado: http://archive.today/gONJ5).

[227] Pizza day 10 anos depois: https://cbsn.ws/2UhKHZb

[228] *NFT - non fungible tokens* existem amplamente desde 2016 com os "Rare Pepe" da *counter party e são registros na blockchains de imagens, videos ou textos que possam ser considerado arte em si mesmos ou prova de propriedade de arte ou outro ativo: NFTs History — From Rare Pepe to Beeple 69 Million Dollar NFT sale:* https://bit.ly/3w6LJ7S *(arquivado: http://archive.today/aPaOG).*

[229] A arte de sonegar: Como milionários usam obras de arte para evitar serem roubados: https://bit.ly/3DoRiDA

[230] *NFTs are Doomed:* https://bit.ly/3h7Zoat (arquivado: http://archive.today/dlHH3).

[231] *NFT* na Liquid: https://elixir.app/

[232] 6 leis de maca: https://twitter.com/noshitcoins/status/1427081434385297415

[233] Com o gabarito e a punção da *stackbit*, ou agulha/prego, também pode furar cartão de crédito/plano velho de plástico, ainda mais discreto, para passar na carteira sem chamariz em metal.

[234] *Plausible Deniability*: https://bit.ly/3xhURrE

[235] Uma ENORME oportunidade judicial existe em responsabilizar o *YouTube/Google* por receber dinheiro de bandidos para anunciar falsos *giveaways*, até mesmo permitindo que robôs fraudem número de curtidas/*views*. O google não é apenas negligente em sua "*due diligence*", como também mama no dinheiro roubado. Eficiente para banir "discurso de ódio" (ideologia contrária a deles) e incapaz de retirar do ar anúncios oficiais de crimes, com os quais eles lucram às custas das vítimas.

[236] *Known Physical Bitcoin Attacks:* https://bit.ly/3AnQmh3

[237] *How to Protect Your Bitcoin from $5 Wrench Attacks:* https://bit.ly/2UhLR6Z (arquivado: http://archive.today/j7wZJ).

[238] *Visions of Bitcoin:* https://bit.ly/3x40XM5 (arquivado: https://archive.vn/3bUve).

[239] Visions of Bitcoin: https://bit.ly/3h7W6Eb

[240] *Why Bitcoin is the Key to Abundance:* https://bit.ly/3AtgEOO

[241] Uma entrevista com F. A. Hayek – 1984: https://bit.ly/3qASzBo (arquivado: https://archive.vn/h1XMz).

[242] Milton Friedman prevê bitcoin em 1999: https://bit.ly/2SPflsO

[243] Peter Thiel prevendo bitcoin em 1999: https://bit.ly/3wc4XJ4

[244] Problema dos dois generais: https://bit.ly/3yjerUh

[245] Ordem cronológica com um link para mais informações detalhadas sobre o gráfico: https://bit.ly/2SLNFVH (arquivado: https://archive.vn/ytlPv).

[246] Fonte: *Money transformed - The future of currency in a digital word F&D - Finance and Development – June 218 FMI- Internacional Monetary Fund:* https://bit.ly/3heT0y3

[247] Nick Szabo, *The History of Money:* https://bit.ly/3wgVQqs

[248] Nick Szabo, *Shelling Out: The Origins of Money:* https://bit.ly/3hfvD7K (arquivado: http://archive.today/e8igf).

[249] Comércio é troca voluntária que eleva valor, em regra, se uma pessoa vende um bem por R$1, para o vendedor ele vale menos de R$1 e para o comprador mais de R$1 - e ambos saem subjetivamente mais ricos da transação.

[250] Degeneração das repúblicas. CAESARISM: THE DECLINE OF THE WEST: https://bit.ly/3dGkvyr

[251] Compra de poder estatal para produção de decisões, políticas e leis para seu benefício direto, como Elon Musk*: Debunking Elon Musk* (a parte 2 é ainda melhor para entender seu histórico fraudulento): https://bit.ly/36c9VeA

[252] *Double eagle:* https://bit.ly/3jTzZTR

[253] 2000 réis: https://bit.ly/3jC2lSh

[254] Fonte: @BTCTimeTraveler *(Twitter).*

[255] Fonte: @anilsaidso *(twitter).*

[256] *Japan central bank loses billions on ETFs, may face annual loss*: https://reut.rs/3x8KXbJ (arquivado: https://archive.vn/3AWTA).

[257] *Swiss Central Bank Holds $129 Billion in Equities, Owns More Public Shares of Facebook Than Zuckerberg:* https://bit.ly/3hkupHa (arquivado: https://archive.vn/gx5TT).

[258] *Debt Traps*, projetos chineses economicamente inviáveis usados como "armadilhas de dívida" para controlar a infraestrutura fundamental e a finanças de países controlados, incluem construção de cidades inteiras no Egito (*NAC*), Indonésia (*Jokograd*), Malásia (*Forest City*) e a Ponte de Itaparica.: https://bit.ly/3wkplrA

[259] *Central banks balance sheets for the BoJ, ECB, Fed, SNB and BoE:* https://tmsnrt.rs/367qrMC (arquivado: http://archive.today/MddeJ).

[260] *Only One Number Mattered to Global Markets in 2020:* https://bit.ly/3AfTWtB (arquivado: http://archive.today/6q8I3).

[261] *1929 versus now: are we headed for the greatest depression?* (Mike Maloney): https://bit.ly/3hdVpZW

[262] O Bug do ouro: https://bit.ly/3ycxPm4 (arquivado: http://archive.today/VYvvw).

[263] Na Venezuela o bitcoin tem ágio altíssimo e ouro não vale nem metade. Ouro sintético colateralizado por cripto já é algo superior a ouro físico em vários aspectos: pode ser facilmente verificado, capitalizado, usado como colateral, alugado e enviado pela Internet.

[264] *Ford Quote:* https://bit.ly/36dtUcO

[265] Carl Menger, "pai da Economia Austríaca", estruturou a vendabilidade através do tempo (durabilidade), espaço (transportabilidade) e escala (divisibilidade): *[THREAD BITCOIN STANDARD*] @MisesCapital (twitter): https://bit.ly/3dz2B0C (arquivado: http://archive.today/iWk9s).

[266] Golpe de bilhões: https://bit.ly/3xlzbuE (arquivado: http://archive.today/ijUUF).

[267] [THREAD OURO - RESERVA DE VALOR]: @rothbarbara (*twitter*)

A desmonetização do Ouro vem sendo desde seu último *rally* na década de 80: https://bit.ly/3AiII7N (arquivado: http://archive.today/3kbr9).

[268] Empréstimo colateralizado em real a partir de 0.69%am: https://rispar.com.br

[269] *Originalmy*: https://originalmy.com

[270]Considerando XAU, onça troy, 31,1035g, a 2000 USD: https://8marketcap.com

[271] Ouro compra 1 leva 2: https://bit.ly/2UVqedf (arquivado: https://archive.vn/K4ePg).

[272] 83 Toneladas em ouro falso em bancos: https://bit.ly/3AdjSpI (arquivado: https://archive.vn/X6d8w).

[273] *World Gold Council*: https://www.gold.org/about-gold

[274] *Venezuela's Bitcoin Birth Proves Crypto Beats Gold in Hyperinflated Economy:* https://bit.ly/3y8qpAc (arquivado: https://archive.vn/x3ySL).

[275] A unidade nativa da Lightning Network é o milissatoshi, equivalente a 0,001 satoshi ou 0,00000000001 BTC (onze casas decimais).

[276] *The Bullish Case for Bitcoin:* https://bit.ly/2UQWnm5 (arquivado: https://archive.vn/K9Knq).

[277] *S2F: Stock to Flow.*

[278] *Para comparar retornos e índices de ativos em BTC:* https://www.microstrategy.com/en/hyperintelligence/asset-vs-btc

[279] Dalio prefere BTC a títulos, que seriam "perda fixa": *Bridgewater's Ray Dalio Says He Prefers Bitcoin to Bonds:* https://bloom.bg/3Aq9DP9 (arquivado: http://archive.today/SgJpT) bitcoin é um ativo com baixa correlação com demais mercados e altos índices de retorno descontados do risco, capaz de elevar lucratividade potencial na composição de carteiras.

[280] Em junho de 2021, Paul Tudor Jones passa a recomendar não 1%, mas agora 5% da carteria em Bitcoin: https://bit.ly/3ymT1p9 (arquivado: http://archive.today/o5r4l)

[281] Como o Bitcoin força o consenso entre os generais bizantinos? https://bit.ly/3w6YOy0 (arquivado: https://archive.vn/cy625).

[282] Falha Bizantina, o que significa? https://bit.ly/3htUCTM (arquivado: https://archive.vn/fG55a).

[283] Prova de trabalho, *Proof-of-Work* (*PoW*). Uma parte de um dado que requer um esforço computacional considerável para ser encontrada. No Bitcoin, mineradores devem encontrar uma solução numérica para o algoritmo SHA-256 que esteja em conformidade com os parâmetros da rede.

[284] Efeito Lindy: https://pt.wikipedia.org/wiki/Efeito_Lindy

[285] Efeito rede: https://pt.wikipedia.org/wiki/Efeito_de_rede

[286] Lei de Gall: http://principles-wiki.net/principles:gall_s_law

[287] Compilação dos melhores links para artigos desmascarando Bitcoin FUD: https://endthefud.org/

[288] *Thirst Trap:* https://bit.ly/36fcX1z

[289] Bitcoin's energy use compared to other major industries: https://bit.ly/3gASSse (arquivado: http://archive.today/ypSeo)

[290] *Bitcoin Energy Consumption Index:* https://bit.ly/3hB2jHs (arquivado: https://archive.vn/WslVC).

[291] *Bitcoin energy use - mined the gap*: https://bit.ly/3hA5YXP (arquivado: http://archive.today/T02oB)

[292] LN 3,7M mais eficiente que VISA: https://bit.ly/2SFtAAn (arquivado: http://archive.today/7GuGT).

[293] *Bitcoin and ESG*: https://bit.ly/3hiPKR8 (arquivado: http://archive.today/7OYuw).

[294] *ESG = Energy Stops Growing*: https://bit.ly/2Ue6KjN (arquivado: http://archive.today/GQfZ7).

[295] 30 anos de *economic warfare* chinês contra ocidente / *Panic As Chinese Skyscraper Wobbles!:* https://bit.ly/2WuzlT9

[296] *Superdollars* da Coréia da Morte / *When North Korea tried to hijack the US dollar*: https://bit.ly/3dG1FHK

[297] Até mídia esquerdista especula se COVID foi fabricada: https://on.wsj.com/3h986oG (arquivado: http://archive.today/1ICtP).

[298] Teoria Crítica Racial e marxismo até nas forças armadas: https://youtu.be/1814HNjVntA

[299] *COVID BIO WEAPON*: https://bit.ly/3x9D9qg *(youtube)* / *Wuhan Coronavirus Lab Leak No Longer a "Conspiracy Theory":* https://bit.ly/3w9ukvk

[300] OMS mentiu dolosamente: *The WHO Knowingly Lied About China:* https://bit.ly/3jyMhkm

[301] Comer carne salva planeta: *Eating less Meat won't save the Planet. Here's Why*: https://bit.ly/3hoxKF4 há tréplica também neste canal a todos os argumentos mentirosos dos ativistas.

[302] Imagens de Bill Gates com mama *(man boobs)* e culote *(love handles*): https://bit.ly/3wb6GP5 (arquivado: http://archive.today/ldcQd).

[303] Focinheiras insalubres e inseguras: https://bit.ly/3AbJDXo (arquivado: http://archive.today/udjs3).

[304] Declaração de Barrington: https://bit.ly/3wbfG6K (arquivado: http://archive.today/ti8fZ).

[305] *Michael Bedford Taylor, University of Washington*: https://bit.ly/2UXJTt3 (arquivado: https://archive.vn/dz0AG)

[306] *Dhruv Bansal*: https://bit.ly/2UXJTt3 (arquivado: https://archive.vn/dz0AG) e https://bit.ly/3h6MqJU (arquivado: https://archive.vn/Glj17)

[307] Gigante norueguesa no setor de petróleo e gás, presidida por Kjell Inge Røkke, um dos dez homens mais ricos da Noruega.

[308] Cartas aos investidores da AKER: https://bit.ly/2V21ss5

[309] *Whitepaper* da Square sobre energia e Bitcoin: https://bit.ly/366Kqva

[310] *Bitcoin Clean Energy Initiative*: https://squ.re/3ktrTzJ (arquivado: http://archive.today/RsbuW)

[311] *A Closer Look at the Environmental Impact of Bitcoin Mining:* https://bit.ly/3uY8ET1 (arquivado: http://archive.today/vB2bU)

[312] *On Bitcoin`s Energy Consumption: A Quantitative Approach to a Subjective Question*: https://bit.ly/3hwHfDP (arquivado: http://archive.today/NHn8M).

[313] Crise energética no Texas: https://bit.ly/3jLNJzX

[314] Lado sombrio da energia solar: https://bit.ly/2Tifu8r (arquivado: http://archive.today/vNTGg).

[315] Usualmente inconstante em sua produção, como solar e eólica.

[316] Desastre alemão: https://bit.ly/3Alrh6g (arquivado: http://archive.today/BspBI).

[317] *Safely Managing Used Nuclear Fuel:* https://bit.ly/3fpK9Yh (arquivado: http://archive.today/tZxf8).

[318] *5 Fast Facts about Spent Nuclear Fuel:* https://bit.ly/3orWhvP (arquivado: http://archive.today/ZhnAW).

[319] *Novaterra*: https://cnb.cx/3juCFa9 (arquivado: http://archive.today/hl6v0).

[320] O *"The Great Reset"* é uma versão reformulada e restrita da agenda de "Desenvolvimento Sustentável" de décadas da ONU ("Agenda 21"): https://bit.ly/3wmPmGE (arquivado: http://archive.today/zu96e). As mesmas políticas e ideias estão contidas no *"The Green New Deal"*, que foi reprovado em 2019 no Congresso dos EUA: https://bit.ly/36iPvAo (arquivado: http://archive.today/Pys9Y).

[321] Fórum Econômico Mundial (FEM) em conjunto com as Nações Unidas (ONU) e o Fundo Monetário Internacional (FMI) / *Meet the World Economic Forum:* https://bit.ly/36ls6yp

[322] O Grande Reset Financeiro Mundial: https://bit.ly/3jKvvyG

[323] Afinal, qual é a desse "Grande Reinício"? https://bit.ly/3dPOAvk (arquivado: http://archive.today/8O8Yg).

[324] Globalista Klaus Schwab: O mundo "nunca" voltará ao normal depois do COVID-19: https://bit.ly/36e7p7w (arquivado: http://archive.today/PDp1p).

[325] *Bitcoin Address:* https://en.bitcoin.it/wiki/Address (arquivado: https://archive.vn/uBmN6).

[326] Para Chaves, Endereços e Carteiras no Bitcoin: diferença entre Chave Pública e Endereço, ver o artigo no *medium* da Rafaela Romano: https://bit.ly/2UfqR10 (arquivado: https://archive.vn/ljQxw) e https://medium.com/@rafaelaromano.

[327] *BIP - Bitcoin improvement proposal* (Proposta de Melhoria do Bitcoin) é um documento para a introdução de novos recursos ou informações no Bitcoin.

[328] Unidades de medida: https://bit.ly/3jFmHdf (arquivado: https://archive.vn/fWidk)

[329] A circulação total em abril de 2019: https://coinmarketcap.com em 27/04/2020

[330] Blog do Nick Szabo: https://bit.ly/3qFZngZ (arquivado: https://archive.vn/454kk).

[331] *Money, blockchains, and social scalability:* https://bit.ly/3hoAthB (arquivado: https://archive.vn/454kk).

[332] *Opendime*: https://opendime.com

[333] *Stackbit*: www.stackbit.me

[334] Acompanhe a "Serie bugs do Bitcoin": https://bit.ly/38eyto4 (Canal do youtube Safersr apresentado por Peter Turguniev, entender a historia dos problemas do Bitcoin e como o a rede tem a capacidade de atrair as maiores mentes do mundo da programação para manter tudo isso "de pé".

[335] Bug de inflação *(CVE-2010-5139)*

[336] *Bitcoin History Part 10: The 184 Billion BTC Bug* (CVE-2010-5139): https://bit.ly/3wm4sfJ (arquivado: http://archive.today/UXsTW).

[337] Duas horas depois da ocorrência do *Common Vulnerability and Exposure 2010-5139*, os desenvolvedores do Core Gavin Andresen e Satoshi Nakamoto estavam no caso, e a transação de 184 bilhões de BTCs foi eliminada do bloco 74638.

[338] Quanto custa fazer um ataque de 51% em cada criptomoeda que utiliza o *PoW:* https://www.crypto51.app/

[339] https://www.bitcoinblockhalf.com/

[340] Gráficos de BTC desde sempre em prata, ouro, US$ e índices disponíveis em *Asset gallery*: https://asset.gallery

[341] Mesquitas de Mamón: https://bit.ly/3wivxQV

[342] Tutorial/experiência de como minerar em casa - *Home mining for non-KYC Bitcoin: https://bit.ly/3mDgpws* (arquivado: http://archive.today/HY2fL)

[343] *HODL*: https://bit.ly/3x5YDUR

[344] Satoshi na época chegou a se opor a *Wikileaks* aceitar BTC, imagine uso por *Silk Road.*

[345] IN 1888/2019: https://bit.ly/3dB9MFz (arquivado: https://archive.vn/kIuuE).

[346] Calculadora do preço médio: https://dcabtc.com

[347] Preço médio de compra, bitcoins dormentes por dia, saldos líquidos em corretoras, *hashrate* e valor movimentado por dia são indicadores (mesmo que consequentes) dos fundamentos do BTC.

[348] Crédito em Reais com garantia em bitcoin: https://rispar.com.br/

[349] Cotações do *lending*: https://defirate.com/btc/

[350]*Skew*: https://analytics.skew.com/

[351] *Florida Teenager Is Charged as 'Mastermind' of Twitter Hack:* https://nyti.ms/3dxK8BB (arquivado: https://archive.vn/WUIBP).

[352] *Colonial Pipeline* paga 90 milhões em *ransom* para nada: https://bit.ly/3AeuKnr (arquivado: http://archive.today/kCZ48).

[353] *Wannacry*: https://glo.bo/3h9V8Y3 (arquivado: https://archive.vn/XzPpJ)

[354] *Wannacry wiki*: https://bit.ly/3h7BOKY

[355] Por que os bancos centrais poderiam emitir moedas digitais? https://bit.ly/3hc12Yo (arquivado: http://archive.today/WhwOD).

[356] Como o advento do Bitcoin pode influenciar o pensamento dos Bancos Centrais: https://bit.ly/3wh6xcY (arquivado: http://archive.today/qXU0J).

[357] *The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies*: https://bit.ly/3h6Yz1s (arquivado: http://archive.today/87Xup).

[358] *FED AND UN think CBDC could kill Banks:* https://yhoo.it/3hs4BsE (arquivado: http://archive.today/fC7GJ).

[359] O fim dos bancos como conhecemos: https://bit.ly/3dPTfOd

[360] “Teimosinha" é a busca automática de ativos nas contas do devedor de forma contínua: https://bit.ly/3h9WulF (arquivado: http://archive.today/7qjoO).

[361] Vide as 10 medidas nazi stalinistas, amplamente defendidas por órgãos aparelhados e militantes, como MPF: https://bit.ly/3y5iHqy (arquivado: http://archive.today/nwMfA).

[362] Arthur Hayes sobre juro negativo e cenários futuros: https://bit.ly/3duqK8v

[363] *MPEX* (*Mircea Popescu Exchange) em 2011 já provava como se poderia negociar futuros, commodities, opções e sínteticos de moedas e ações - embora o site fosse apenas um prova de conceito e os volumes fossem pífios:* http://mpex.biz/faq.html

[364] *Satoshi Dice*: https://en.bitcoin.it/wiki/Satoshi_Dice

[365] *Piper Wallet* de 2015 gerava e imprimia chaves *offline*: https://bit.ly/3hgE4Qg *hardware wallets* mais modernas como MK3 da *Coldcard* geram transações *offline*.

[366] BOLSONARO2022: https://bit.ly/3haDsLP (arquivado: http://archive.today/GpPrj).

[367] Solução de mercado para libertar a Venezuela: https://bit.ly/3sOr3RO (arquivado: http://archive.today/dXojH)

[368] Candidato no Brasil a ser o *APP* oficial é o *Nubank* que conta com participação do *deep state* e da ditadura chinesa desde 2018 através da *Tencent* (dona do WeChat)

[369] Utilize o site https://hive.one, um serviço que faz um *rank* sobre as principais personalidades do mundo *crypto.*

[370] *DYOR* entre Posteo, Protonmail, Tutanota e outros: https://zapier.com/blog/secure-email/

[371] Democratas já tem listas públicas para expurgos e reeducação: https://bit.ly/3hpLFut (arquivado: http://archive.today/8gXFG).

[372] *"Como o governo e as big techs* estão doutrinando você” : NOVO, Bolsonaro e “moderados” são instrumentos progressistas: https://bit.ly/3hbiah8

[373] *Everything bubble*: https://bit.ly/2Ugmd2F

[374] *Financial markets:* https://bit.ly/2Uk3O51

[375] *Dissection of Bitcoin’s multiscale bubble history:* https://doi.org/10.1098/rsos.180643 (arquivado: https://archive.vn/trmp9).

[376] Lei de Metcalfe: https://bit.ly/3jCCidG

[377] *Aimstone explica estimativa de Breedlove:* https://bit.ly/3wfIH14

[378] Gráfico atualizado diariamente (@Ecoinometrics): https://ecoinometrics.substack.com/

[379] Ouro a 50k USD em 2022 / *Can Gold Hit $50,000 By 2022? (Expert Says YES!):* https://bit.ly/3qMtQdy

[380] 5 fases do BTC: https://bit.ly/3wcPMiK

[381] Peter Thiel afirma que bitcoin é arma estratégica e roga que EUA pare de vender os *tokens* apreendidos: https://bit.ly/3jvaibX (arquivado: http://archive.today/c9kMi).

[382] *Tether Dollar, USDT:* https://bit.ly/3hsbHxi

[383] CME manipulation: https://bit.ly/3qEQTqs

[384] Mercado provocando maximum pain no varejo: https://bit.ly/3w5hv52

[385] Considerando XAU a 1900 USD.

[386] *All the world's money and markets in one visualization*: https://bit.ly/3hadMyN (arquivado: https://archive.vn/7Ee0I) só para se ter uma noção de como esses números estão defasados e a impressão de moeda medonha, nessa publicação (maio de 2020) existiam 2095 bilionários, em maio de 2021 já eram 2755, segundo o *ranking* da Forbes: https://bit.ly/3dRYSvl

[387] Estimativas indicam mais de 199.000 toneladas de ouro em 2019: https://bit.ly/3wdernv

[388] Inflação do ouro em 2,5% aa na década: https://bit.ly/3jDhrXB (arquivado: http://archive.today/X5xGU) e inflação do bitcoin em 2021 é de 1,8%.

[389] Conta detalhada: https://bit.ly/3AdiQKt

[390] Quantos satoshis existem por pessoa no mundo? https://satoshisperperson.com/

[391] 24 (horas por dia) * 6 (blocos por hora) * 6,25(BTC por bloco)

[392] *Grayscale's 654,885 BTC:* https://bit.ly/2UPhh52

[393] Entidades que possuem bitcoin em seus balanços: Bitcoin Treasuries: https://www.buybitcoinworldwide.com/treasuries/

[394] *Tesla still has 38300 BTC*: https://bit.ly/2ToZcdG

[395] *Gartner Hype Cycle:* https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

[396] *Bitcoin is not too volatile:* https://bit.ly/3zs7bqq

[397] *Bitcoin Price Forecast:* https://bit.ly/2TuzLHH (arquivado: https://archive.vn/5Hlim).

[398] *Podcast* de Stephan Livera: https://stephanlivera.com/episode/2/

[399] Lei de Gresham: https://bit.ly/3jDlK5d (arquivado: https://archive.vn/l5co6).

[400] 5 fases do BTC: arquivado: http://archive.today/NZp7q

[401] GBTC | Grayscale Bitcoin Investment Trust: https://grayscale.com/products/grayscale-bitcoin-trust/

[402] *Ranking* de empresas que estão entesourando bitcoins: https://bitcointreasuries.org/

[403] QBTC11 ou HASH11? https://bit.ly/3AnUgqd

[404] Psicologia dos Ciclos emocionais de Mercado: https://bit.ly/3dIXZ7Y (arquivado: https://archive.vn/DihRt).

[405] *Mayer multiple:* https://mayermultiple.info/

[406] S*tock to Flow*: https://bit.ly/3hzDn3c

[407] Bitcoin em 2020 é Internet em 1997: https://bit.ly/3qDl7Kq

[408] *Hyperbitcoinization:* https://bit.ly/3AjqS4A (arquivado: https://archive.vn/4P085).

[409] Super ciclos: https://bit.ly/3dGFsJA

[410] Um problema atual é o excesso de crédito, a maioria das grandes empresas hoje são zumbis: só existem graças a juro negativo. Se o juro subir ao normal histórico, muitas empresas somem.

[411] Volatilidade do bitcoin está menor no *halving*: https://bit.ly/3xcYn6C (arquivado: https://archive.vn/JsXwl).

[412] *Programming Bitcoin: https://amzn.to/3Auqbpc*

[413] *@real_vijay Twitter*.

[414] Debates e *roadmaps* históricos: https://bit.ly/3h70JOO (arquivado: https://archive.vn/sNHXb).

[415] *Bitcoin Roadmap to 2025*: https://bit.ly/3dx8n2w

[416] *Github*: https://bit.ly/3AdpDUt

[417] *BITCOIN BIPs* https://github.com/bitcoin/bips

[418] *Blockstream*: https://blockstream.com/

[419] *Liquid*: https://liquid.net/

[420] *RSK*: https://www.rsk.co/

[421] O que está acontecendo no ecossistema Lightning Network: https://bit.ly/3gYiboj (arquivado: http://archive.today/3s2pP)

[422] Fonte: inmainnet – malhas da rede LN. / Acompanhe o crescimento - *Lightning Network Search and Analysis Engine:* https://1ml.com/

[423] https://bit.ly/3sTnf1T

[424] *Schnorr signature:* https://bit.ly/3yfXsSM

[425] *Taproot Is Coming: What It Is, And How It Will Benefit Bitcoin:* https://bit.ly/2Tr5Xf9 (arquivado: https://archive.vn/jmELU).

[426] *What is the Bitcoin Taproot upgrade?* https://bit.ly/3jHXO0r (Taproot uses a structure called Merkelized Abstract Syntax Trees)

[427] Fungibilidade é o atributo pertencente aos bens móveis que podem ser substituídos por outros da mesma espécie, qualidade e quantidade. Ex.: O dinheiro é o bem fungível por excelência, dado que, quando se empresta uma quantia a alguém (por exemplo, R$100,00), não se está exigindo de volta aquelas mesmas cédulas, mas sim um valor que pode ser pago com quaisquer notas de Real (moeda).

[428] Trilema da escalabilidade: https://bit.ly/3wgAyJC

[429] *Finney Bitcoin banks*: https://bit.ly/3ycUzSP

[430] *Nick Szabo btc layers (twitter):* https://bit.ly/365H2jV

[431] *Lightning Network Search and Analysis Engine: https://1ml.com/*

[432] Os 195.875 WBTC nem consideramos na conta nem os *wrapped BTC em outras redes como Tron que só aumentam as distorções do coin market cap* para arguir pela "perda de dominância". A busca de *tokens* sintéticos em *shitcoins* para economizar em custos de transações representa riscos operacionais compostos - ganhar de colher para perder de balde.

[433] *Drivechain:* https://www.drivechain.info/

[434] *Statechains:* Non-custodial Off-chain Bitcoin Transfer: https://bit.ly/3hnuZUt

[435] *Private & scalable smart contracts for Bitcoin and Lightning Network:* https://rgb-org.github.io/

[436] Impervious: https://www.impervious.ai/

[437] *Stacks:* https://www.stacks.co/

[438] https://twitter.com/100trillionUSD.

[439] https://medium.com/@100trillionUSD.

[440] *Fermions Flows (FF) Whale Model:* https://bit.ly/3qH4ihN (arquivado: https://archive.vn/qNLEo).

[441] Comparações e definições *(Bitcoin Price Models*): https://bit.ly/3dF8xFp

[442] *Bitcoin price and its marginal cost of production:* https://arxiv.org/pdf/1805.07610.pdf

[443] Ray Nasser – China e seu erro de 1 trilhão de USD: https://bit.ly/3Do6P6o

[444] *Bitcoin's Cost of Production: https*://bit.ly/3sVfZCo

[445] *Bitcoin Price Forecast: https://bit.ly/3qHftXz* (arquivado: https://archive.vn/5Hlim).

[446] Fonte: www.visualcapitalist.com

[447] https://99bitcoins.com/bitcoin-obituaries/

[448] Quais os Impactos da Computação Quântica para os Bitcoins: https://bit.ly/36acHkp (arquivado: https://archive.vn/WZpH9).

[449] Fonte: www.administradores.com.br

[450] Talibã significa "estudante", para quem tiver dúvidas de que instrução formal não "melhora" pessoas intelectual ou moralmente. *Origins of Taliban:* https://www.youtube.com/watch?v=zzBVvyBWDD4 O Antigo Testamento já reconhecia que "estudar demais é enfado" e que "não há limites para fazer livros" (papel aceita tudo), no Eclesiastes 12:12.

Table of Contents

Revolução Satoshi

A Revolução das Esperanças Crescentes

Revolução Satoshi

A Revolução das Esperanças Crescentes

Escrito por
Wendy McElroy

1ª edição

Sumário

Agradecimentos

Primeiro e antes de tudo, eu gostaria de agradecer a Roger Ver pela confiança que ele depositou em *A Revolução Satoshi* e pela generosidade com a qual ele trata a mim e a todos os outros com quem ele trabalha. Ele é o tipo mais raro de visionário; um que traduz sua visão na realidade.

Pessoas demais no Bitcoin.com ajudaram na serialização de uma versão inicial de *A Revolução Satoshi* para que eu possa listá-las, mas algumas não podem passar sem menção. Mate Tokay é um coordenador magistral para todas as coisas no bitcoin.com e o responsável por preservar tanto o contexto amplo da operação bem como suas minúcias. As décadas do Editor-Chefe Nanok Bie no jornalismo foram inestimáveis. Marcel Chou é um editor paciente que se tornou um amigo e porta-voz confiável. Aqueles que eu cheguei a chamar de "The Bitcoin Guys", nem uma vez tentaram influenciar as teorias sendo testadas e as hipóteses sendo publicadas. Sou grata a todos eles.

Jeff Tucker, autor do Prefácio, tem sido para mim um associado altamente estimado por muitos anos; ele não poderia ter sido mais encorajador com os artigos na medida em que eles apareceram. Para seu crédito, Jeff captou mais rápido do que eu as implicações extraordinárias que as criptomoedas têm para a liberdade. Minha evolução nesse entendimento também possui uma dívida com uma quantidade muito numerosa de pessoas para listar. O mais proeminente entre eles é o notável advogado de propriedade intelectual Stephan Kinsella e o Presidente do Satoshi Nakamoto Institution, Michael Goldstein.

Eu tive outra sorte grande durante *A Revolução Satoshi*. Repentinamente, a Dra. Peri Dwyer-Worrell me mandou um e-mail com uma oferta para revisar meus artigos. Eu sempre fui indiferente em assuntos tais como a colocação de vírgulas, carregando comigo a crença de que apenas as ideias são importantes. Peri provou que eu estava errada e, no processo, ela me fez uma escritora. Eu estou muito agradecida por finalmente ter cuidado com a pontuação e por conhecer essa elegante mulher.

Nenhuma dedicatória estaria completa sem uma expressão de meus agradecimentos eternos a Bradford, meu marido, que é o pilar indispensável para tudo o que eu faço.

Prefácio

O mundo tem precisado desse livro para que tenhamos a visão geral da revolução que está ocorrendo, e Wendy McElroy é a pessoa exata para escrever isso. Seu trabalho tem sido imerso na história da liberdade e da luta contra o controle autoritário. Ela traçou essa luta desde o século XIX até o presente, tendo escrito artigos pioneiros e livros contemplando a amplitude da experiência humana. Em *A Revolução Satoshi*, ela voltou a atenção dela ao que estou convencido ser uma das inovações mais memoráveis da história: criptomoedas, ativos e serviços relacionados. Ela explica como, em nosso próprio tempo, essa tecnologia pressagia mudanças fundamentais, grandes mudanças, na relação entre o indivíduo e o estado. Nos últimos dez anos – historiadores futuros notarão isso – observamos a criação de uma nova arquitetura monetária e financeira que poderá servir como uma substituição para tudo que tem sido conhecido e usado no tempo de vida de todas as pessoas hoje presentes.

Experienciamos um dinheiro seguro e útil que funciona em todo o mundo, não é conectado ao estado, e não precisa do atual sistema bancário. O mesmo sistema pode servir como substituição a todo sistema atual de pagamentos que usam moedas nacionais. Esse dinheiro é uma criação puramente mercadológica que adiciona às funções de contabilidade e de reserva de valor uma característica adicional: ser também um meio de pagamento global peer-to-peer.

Uma década atrás, até mesmo teóricos de alto nível disseram que isso não poderia acontecer. E então aconteceu.

Vimos a criação de um sistema de contratos inteligentes, que pode gerenciar um vasto número de acordos, comprometimentos e interações humanas. Até mesmo pessoas que aceitaram que o Bitcoin era real duvidaram que a Ethereum poderia alcançar isso. Mas isso aconteceu de qualquer forma.

Nós até observamos como esse sistema se tornou um instrumento para levantar capital e substituir as funções de empréstimo tradicionais. Três anos atrás, isso era meramente uma ideia especulativa. Então isso se tornou uma realidade de cem bilhões de dólares, e novas formas de capital estão sendo levantadas através da tokenização.

Aparentemente do nada, temos agora todo um conjunto de tecnologias que poderiam concebivelmente deslocar e até mesmo substituir a moeda nacional, opções de pagamento tradicionais, e até mesmo mercados de capitais regulados, e trazer algo novo.

Você está lendo isso e pensando: aqui vamos nós de novo com o cripto-utopismo. Mas esse é o pulo do gato: não é mais apenas teoria. Essas tecnologias existem, ao vivo e em cores, mesmo que estejam em seus estágios iniciais. É por isso que há tantos bitcoiners por aí que falam tão exuberantemente sobre o futuro. Eles já experimentam isso. Eles são motoristas de Maseratis em estradas cheias de Ford T's, e eles sabem disso. Uma melhoria do status quo que é tão impressionante que não será suprimida.

Você pode não ter usado qualquer uma dessas novas tecnologias. E está tudo bem. Com todas as falhas do atual sistema, as antigas estruturas cumprem seu trabalho. Na medida em que não há uma grande crise no sistema, as pessoas confiam nele. Não há razões fortes para mudar, mesmo que o novo sistema seja mais seguro, mais rápido, mais democrático, mais inclusivo e menos arriscado e comprometedor da privacidade individual. Ainda assim, o antigo sistema goza do ímpeto que vem a partir do efeito manada. Todo mundo confia no antigo sistema, então você continua confiando nele também.

A Regulação é a Chave

Há outro fator que está atrasando a mudança do antigo para o novo. As regulações estão tentando forçar a nova tecnologia a se comportar como a tecnologia antiga. Nos Estados Unidos, para comprar Bitcoin ou qualquer criptomoeda, você precisa cumprir com regulações know-your-customer, cedendo cada detalhe sobre a sua pessoa. Qualquer dinheiro que você faça de movimentos dos preços em ascensão em um novo ativo precisa ser registrado e você precisa pagar impostos sobre ele. Companhias que desejam prestar assistência no onboarding e no offboarding de cripto para moeda fiduciária têm de se registrar no governo como casas de câmbio. E, com as funções de alavancamento de capital da tecnologia blockchain, os reguladores estão ameaçando acabar com todas e fazê-las se comportar como títulos tradicionais.

Eu assisti enquanto essas regulações, gradualmente impostas e arbitrariamente reforçadas, introduziram um elemento de medo em uma

tecnologia sem medo, distorcendo o setor e fazendo dele menos inovador e menos competitivo. Toda vez que um novo uso das redes distribuídas é revelado e começa a se espalhar, alguns mandachuvas surgem do alto para advertir sobre a conformidade com leis de décadas atrás designadas para diferentes tecnologias.

Os consumidores ficam com medo, e a experiência de usuário final não é aprimorada o tanto quanto ela poderia ter sido na ausência de tantos custos de compliance. Eu vi o quanto a incerteza legal fez com que os mercadores e os consumidores perdessem acesso a uma variedade de serviços. Eu vi empreendedores interromperem seus planos, esperando algum édito administrativo vindo de Washington, DC.

O quão mais avançados estaríamos no caso da ausência dessas regulações? É impossível ver as inovações que não experienciamos. Sabemos apenas que as coisas seriam diferentes. Mas uma vez que você considera o quão diferente seriam, a realidade se torna algo além do incrível. E ainda não chegamos nisso.

Quanto Tempo Vai Demorar?

Considere o que acontece quando o poder é usado para parar o progresso de uma nova tecnologia. Isso realmente funcionaria no longo prazo? Para responder à questão, temos de nos engajar nos contrafactuais.

Imagine se os governos na Europa tivessem se empenhado para parar a prensa. E se as cidades ao redor do mundo tivessem banido os automóveis? Qual teria sido o destino das ferrovias, da iluminação doméstica e do encanamento fechado se interesses especiais houvessem sido suprimidos em favor das tecnologias prevalecentes?

Podemos apenas especular, porque nada disso realmente aconteceu. É verdade que nem todo mundo recebeu bem a prensa. Escribas em monastérios se preocuparam com o futuro de seus talentos. Algumas pessoas perguntaram se a velha fé poderia sobreviver às pessoas tendo acesso aos textos antigos. Mas, em geral, o advento da prensa foi visto como uma inovação bem-vinda. Assim também se deu com a combustão interna, eletricidade e encanamento. Algumas pessoas ficaram receosas em adotar elas, é claro, mas os governos em sua maioria deixaram a inovação acontecer.

E se eles não tivessem? Alguém realmente acredita que essas inovações poderiam ser paradas e não meramente atrasadas? Eu penso que

não. Há casos na história em que garantias de monopólios por parte do governo retardam competidores de adentrarem no mercado com melhorias. Isso aconteceu com os navios a vapor na Inglaterra, com os aviões nos EUA, e com algumas aplicações de software nas últimas décadas. Mas esses retardamentos são temporários; patentes expiram e a história vai para frente.

Regulações são diferentes. Os empreendedores têm de inovar ao redor delas. Os mercados cinza e negro emergem. Aventureiros encaram as autoridades. Mas, eventualmente, alguém cede. Considere, por exemplo, os resultados caso todo lorde e barão na Europa do século XII tivesse banido a ferradura. Você acha que isso teria parado a implementação dessa tecnologia por séculos? Altamente duvidoso, e a razão é fundamental: ideias são mais fortes que governos. Eventualmente, os custos de imposição excedem vastamente os benefícios da classe governante existente.

Um Mundo Criptonizado

À luz do que temos visto nos últimos dez anos, aqui está um experimento mental com o qual eu venho brincando. Ele ocorreu a mim numa divagação, enquanto meu advogado tributário estava explicando-me profundamente sobre eventos tributáveis nos acordos cotidianos com cripto. Eu estava considerando o quão incompatíveis eram essas imposições com uma tecnologia que emergiu de e opera dentro de uma estrutura de perfeita liberdade.

Algumas legislações entenderam isso. O Wyoming, por exemplo, isentou a cripto de toda tributação, definiu certos tokens de um modo que faz deles isentos de leis de títulos, e fizeram provisões especiais para formas corporativas que são distribuídas, entre outras mudanças. A legislação fez o seu melhor para tornar o estado atrativo para essa nova indústria.

Agora, deixe-nos entrar no campo da fantasia. Digamos que o congresso dos EUA passe uma legislação que isente toda criptomoeda, todo criptotrading e criptoativos de toda tributação e regulação. A legislação estabeleceria laissez-faire completo nesse setor, enquanto todo o resto no mundo normal (o dólar, o FED, a SEC, o Tesouro, e todo o resto que conhecemos) permaneceria o mesmo.

O que você acha que aconteceria? Dez anos atrás, se o Congresso tivesse feito a mesma coisa, pouca coisa teria mudado, obviamente. A

tecnologia não existia, e nós realmente não sabíamos que ela poderia existir.

O que aconteceria hoje se todas as intervenções ao redor dessa tecnologia fossem repelidas? Você não seria mais punido por comprar e vender em cripto, emitir novos tokens, desenvolver novos aplicativos em plataformas de contratos inteligentes, inovar novos sistemas de pagamentos e assim em diante. Companhias poderiam tokenizar em vez de vender ações. Os negócios poderiam pagar em cripto e fazer sua contabilidade em cripto e evitar qualquer penalidade. Considere com cuidado: você poderia manter um terço a mais dos seus ganhos justos simplesmente mudando para uma tecnologia melhor.

Quanto tempo levaria para a criptoeconomia substituir todo o resto? Se essa mudança legislativa realmente acontecesse – e não, obviamente não vai – poderíamos observar o deslocamento geral dos sistemas econômicos e financeiros do velho mundo para os sistemas do século XXI, e talvez isso acontecesse muito mais cedo do que qualquer poderia esperar, talvez de 12 a 48 meses, dado que a infraestrutura da cripto poderia escalar a tempo de satisfazer a nova demanda.

Forçando o Passado no Presente

Agora, se esse experimento mental estiver correto, há algumas implicações poderosas. Isso sugere que o mundo financeiro e monetário, tal como existe hoje, está sendo mantido de pé pela força que está nos prendendo aos velhos modos. Essa força está impondo limitações e ineficiências; ela está literalmente mantendo uma vasta infraestrutura no lugar daquilo que de outro modo cessaria de dominar ou até de existir, e impedindo o início de um novo modo de viver. E esse novo modo não é somente sobre comprar e vender. Tão central para nossas vidas públicas são a moeda nacionalizada e os mercados de capital regulados que o advento de um mundo criptonizado mudaria fundamentalmente a relação do indivíduo com o estado.

Estaria eu errado em estar maravilhado com essa percepção?

Manter um sistema vasto vivo apenas pela força não me parece tão sustentável no longo prazo. Se você possui um conjunto massivo de tecnologias que estão esperando para assumir o controle e estão apenas sendo atrasadas por meios puramente artificiais, esse cenário não parece sustentável dada a improbabilidade de que o passado possa para sempre

ser preservado. O futuro não pode para sempre ser adiado mesmo pelos governos mais poderosos do mundo. Eventualmente as ideias vencem.

Wendy McElroy, a partir de seus estudos passados de história e de seu mergulho profundo na cripto-tecnologia, entende o poder dessas ideias. O Bitcoin e tudo que é relacionado a ele estão entre as ideias mais revolucionárias da história. Ela demonstra como eles vão transformar para melhor a estrutura da economia, da política, e das relações humanas num geral. Ir daqui para lá requer o entendimento mais amplo possível do que está acontecendo. McElroy é a guia expert e erudita pela qual estávamos esperando.

Jeffrey A. Tucker é Diretor Editorial do American Institute For Economic Research e antigo Diretor de Conteúdo pela Foundation for Economic Education. Ele é parceiro de gestão da Vellum Capital: Blockchain Financial Management, fundador da Liberty.me, Membro Honorário Distinto do Mises Brasil, conselheiro econômico da FreeSociety.com, companheiro de pesquisa no Acton Institute, conselheiro político do Heartland Institute, fundador da CryptoCurrency Conference, membro da bancada editorial da Molinari Review, um conselheiro para a desenvolvedor de aplicativos blockchain Factom. Ele é o autor de milhares de artigos na imprensa acadêmica e popular e é autor de oito livros em oito línguas, o mais recente sendo *The Market Loves You*. Ele fala amplamente sobre economia, tecnologia, filosofia social, e cultura.

"Você nunca muda as coisas lutando contra a realidade existente. Para mudar algo, construa um novo modelo que faça o modelo existente obsoleto."
– R. Buckminster Fuller

A revolução de 2009 passou despercebida pela maioria das pessoas porque ela foi pacífica, ordenada, e tecnologicamente arcana. Em 2009, Satoshi Nakamoto lançou um software de código aberto por meio do qual transferências peer-to-peer de riqueza digital, chamada bitcoins, cintilaram através de um registro imutável e transparente, chamado blockchain.

O modelo mais conhecido de revolução é a derrubada de um governo opressor por meio de uma revolta popular. Mas a dura realidade da história é que outro governo quase inevitavelmente surge como uma substituição – um governo tão elitista e brutal quanto seu predecessor. O modelo Satoshi de revolução é diferente. Ele pacificamente faz com que o sistema antigo se torne irrelevante ao superá-lo através de uma nova tecnologia e de uma moeda privada diferente de tudo antes visto. A criptomoeda se move ininterruptamente pelo mundo sem estados ou fronteiras, obedecendo apenas aos comandos de indivíduos que escolhem fazer acordos uns com os outros. Transferências são pseudônimas com substancial privacidade providenciada por algoritmos de encriptação e por funções hash. A blockchain é imutável e visível para todos, o que faz dela imune à corrupção. Resistente a manipulação e a inflação pelo governo, a cripto não serve elites poderosas às custas das pessoas comuns. O bitcoin, a cripto, em geral, é o dinheiro do povo. (Nota: O Bitcoin com b maiúsculo denota tanto a moeda quanto a blockchain; bitcoin denota a moeda).

Em um instante, com a primeira faísca de transferência, o mundo mudou para sempre.

Liberdade Versus Poder

Os indivíduos subitamente tiveram a arma de autodefesa que estava faltando no arsenal deles – uma arma que era necessária para vencer o que o economista austríaco Murray Rothbard chama de "o grande conflito que é travado eternamente entre a Liberdade e o Poder". Os indivíduos ganharam uma moeda privada viável que os permitiu controlar suas próprias riquezas e se tornarem seus próprios bancos – serem "selfbanks". Finalmente houve um caminho prático para longe da moeda fiduciária manipulada e das instituições financeiras corruptas que formam a base do poder estatal. (As palavras "estado" e "governo" são usadas intercambiavelmente neste livro).

O Bitcoin chegou no momento certo. Apenas dois anos antes, o monopólio monetário causou a crise financeira de 2007-2008 em todo o globo. O Bitcoin e a blockchain ofereceram aos indivíduos um sistema melhor – um que serviu às necessidades deles, não àquelas da elite, e prometeu a independência financeira e controle, os fundamentos da autonomia.

Em sua massiva obra *Conceived in Liberty* (Volume 2), Rothbard apresenta uma visão ampla do porquê dessa libertação ser essencial. Ela não é somente "um grande bem moral em si mesmo", mas também "a condição necessária para o florescimento de todos os outros bens pelos quais a humanidade presa: a virtude moral, a civilização, as ciências e as artes e a prosperidade econômica". Sem uma moeda privada e sem um sistema bancário baseado na Liberdade, não no Poder, o potencial humano estava mutilado.

Até chegar o Bitcoin, entretanto, poucos pré-requisitos de liberdade receberam tanta atenção de ativistas políticos modernos quanto a necessidade por uma moeda privada e por um sistema bancário privado que é acessível a todos. Os guerreiros da liberdade marcharam e morreram sob bandeiras nas quais se liam LIBERDADE, VERDADE e JUSTIÇA. Em nenhuma bandeira que eu me lembre lia-se DINHEIRO PRIVADO, SELF-BANKING, mesmo que esses mecanismos fossem essenciais para cumprir a maioria dos outros objetivos na vida.

(Nota: Dinheiro possui três usos tradicionais: é um meio de troca, uma reserva de valor, e uma unidade de conta. A cripto pode servir às três funções, mas a discussão aqui é limitada à moeda (currency) – o dinheiro em circulação como um meio de troca).

A autonomia econômica é a rocha matriz da libertação sem a qual outros direitos se tornam problemáticos. A liberdade da expressão é irrelevante para um homem morrendo de fome. A liberdade de associação

soa vazia para uma mulher que precisa aguentar abuso físico para alimentar seus filhos. O Devido Processo Legal é irrelevante para alguém que não pode arcar com os medicamentos requeridos para viver mais um dia. A necessidade fundamental para todo ser humano é prover a sua própria sobrevivência. Somente então pode a libertação se seguir, junto "da virtude moral, da civilização, das artes e das ciências".

Por anos, a visão política do indivíduo ou do time conhecido como Satoshi Nakamoto escapou ao radar público. Desenvolvido por cripto-anarquistas e sem ser amparado por decretos do governo ou pela atenção da mídia, as autoridades do estado não notaram o fenômeno, aquelas que o notaram desdenharam dele. Eles notam agora, e seus sorrisos sádicos desapareceram de suas faces. Bancos e negócios agora avidamente adotam e adaptam a blockchain porque eles reconhecem seu incrível poder como ferramenta. Há uma pressa por patentes no que já foi uma comunidade de código aberto. Traders são presos por não serem licenciados. Corretoras são atacadas por não se adequarem à papelada exigida em relação aos consumidores. Os governam clamam para regular a moeda para que se possa controlar não somente seus lucros, mas também o perigo que ela acarreta para seu monopólio sobre o dinheiro.

Rothbard observa, "[A Liberdade] tem sempre sido ameaçada pelas intrusões do poder, o poder que busca suprimir, controlar, aleijar, tributar e explorar os frutos da liberdade e da produção." O poder é também ameaçado pela liberdade porque as duas dinâmicas gozam de uma relação inversa; isto é, enquanto uma cresce, a outra afunda.

Sem dúvida que a visão de Satoshi da libertação individual através da autonomia financeira está sob ataque. Os ataques incluem:

- As criptomoedas são ditas como sendo instrumentos meramente financeiros e como nada sobre as quais se deva estar politicamente entusiasmado. Chamá-las de instrumentos de autodefesa em uma batalha entre Liberdade e Poder é considerado "nonsense anarquista", e a discussão sobre o assunto sequer ocorre.
- Apenas criminosos precisam de privacidade financeira, é dito. Usuários de cripto são traficantes de drogas, sonegadores de impostos, traficantes sexuais e outros similares. De outro modo, por que iriam resistir a se reportarem ao governo? A acusação intimida alguns usuários a permanecerem silenciosos por medo de serem considerados criminosos *a priori*.

- Sem regulação, fraude massiva é dita inevitável. Essa reivindicação diverge a atenção da fraude massiva do sistema fiduciário e do centralismo bancário.

As afirmações precedentes são exemplos dos gravetos que são usados para bater e desacreditar a cripto. Nenhuma delas são válidas, mas muitas são amplamente acreditadas. E as crenças públicas tendem a ser traduzidas em lei sempre que convém ao estado fazer isso.

O ataque mais perigoso à cripto, entretanto, é a "cenoura" – a promessa de respeitabilidade. Até mesmo a comunidade cripto é suscetível a essa tentação. Defensores querem que a blockchain e a cripto sejam tão difundidas quanto possível. Os principais defensores querem aceitação para expandir sobre uma base indivíduo-por-indivíduo, negócio-por-negócio, com todas as interações sendo voluntárias e extralegais. Outros estão menos preocupados com o voluntarismo; eles acreditam que suas reservas e investimentos irão elevar-se em valor se os governos e outras instituições de monopólio se tornarem usuários ou garantidores de segurança. Para esses usuários, a respeitabilidade é a chave para o aumento dos lucros e lucro é tudo. Eles veem defensores que falam sobre a liberdade como obstáculos, instrumentos ou ambos.

Infelizmente, "respeitável" é frequentemente visto como sinônimo para "sancionado pelo estado", quando na verdade os dois termos deveriam ser antônimos. O Bitcoin era necessário precisamente porque instituições do governo e parceiras dele, tais como bancos centrais, são vergonhosas; elas saqueiam as pessoas comuns até os trapos e ossos através de manipulação de moeda, inflação, regulação obstrutiva, impostos e outras artimanhas. As elites botam as pessoas para fora da prosperidade através de licenças, patentes, crédito artificial, restrições de investimento, monopólios e outros obstáculos auto servientes.
Os governos são o problema; eles não são a solução e eles nunca serão. "Sancionado pelo estado" deveria significar "desgraçado", não "respeitável".

Um insulto acrescentado para buscar a sanção do estado é a clara implicação de que a liberdade não é respeitável, que liberdade e respeitabilidade são, de algum modo, antagonistas e requerem o estado como um árbitro. Isso é uma falsa e perigosa dicotomia porque o oposto é verdadeiro, e isso dá ao estado o ponto de apoio por meio do qual se

expande, como sempre acontece. Nada é mais respeitável do que a paisagem de seres humanos fazendo acordos pacificamente uns com os outros visando a vantagem mútua. O que o governo injeta numa sociedade livre é violência ou a ameaça de violência, a qual é o fim da liberdade e da sociedade civil.

As apostas são altas, tanto para a Liberdade quanto para o Poder. Para a Liberdade: Privatizar a sua própria riqueza significa que indivíduos privatizam a vida deles e determinam os termos a partir dos quais eles vivem. Para o Poder: Os governos e as instituições financeiras perdem seu monopólio sobre o dinheiro e sobre a riqueza sem os quais eles são impotentes.

Está na natureza do Poder endurecer suas amarras sempre que ameaçados. O poder irá tentar centralizar, regular, banir ou, de outro modo, dominar as moedas digitais e a blockchain. As tentativas irão falhar, em parte por causa da natureza descentralizada da tecnologia, mas uma grande quantidade de dano pode ser infligida por um estado que falha. A tecnologia não pode ser parada, mas alguns dos indivíduos que a usam podem ser perseguidos, aprisionados e quebrados. A proteção mais certa da vítima é manter clara a visão original de Satoshi sobre a cripto e não se desviar dela.

A Revolução sem Sangue

Essa é a imagem quintessencial da revolução política. Camponeses famintos invadem a Bastilha porque a opressão os moveu para além dos limites da resistência humana. Mas, e se essa imagem estiver errada? Ou lamentavelmente incompleta? E se as forças mais revolucionárias no mundo não forem a fome e o desespero, mas sim a esperança e a oportunidade?

A frase e a dinâmica que captura a última visão é chamada de “a revolução das esperanças crescentes”; ela descreve a promessa mais rígida da revolução Satoshi. O termo tornou-se popular depois que a Segunda Guerra Mundial desestabilizou governos ao redor do globo, com os antigos regimes e sistemas políticos colapsando. A política abomina um vácuo. Especialmente no que era até então chamado de o Terceiro Mundo, as pessoas comuns começaram a acreditar que a vida delas poderia melhorar através de seus próprios esforços. A “revolução das esperanças crescentes” se refere a uma situação na qual um aumento na prosperidade e na liberdade faz as pessoas acreditarem que elas podem

criar uma vida melhor para elas mesmas e para a família delas. Elas não só agem para fazer isso, mas elas também demandam o espaço para respiração política para conseguir mais. Elas têm fome por independência e prosperidade. As esperanças crescentes se tornam uma engrenagem do "populismo" no melhor sentido da palavra.

As autoridades já há muito sabem que um povo oprimido obedece porque eles acreditam que não há alternativa viável. As pessoas acreditam que nenhum ato de resistência pode melhorar a vida delas, então elas mantêm o status quo, por mais sombrio que ele possa ser. A "cinzidade", a conformidade e o medo são os amigos dos regimes totalitários que querem suprimir qualquer faísca de não conformidade ou de criatividade, porque a centelha expressa a escolha individual e a inovação. A centelha não pode ser controlada. Isso é verdade para a esperança. Pessoas esperançosas agem para controlar as suas próprias vidas porque elas vislumbram a possibilidade da libertação e da prosperidade – dois lados da mesma moeda. O sociólogo do século XIX Alexis de Tocqueville observou que a Revolução Francesa foi mais forte em áreas da França onde o padrão de vida havia continuamente evoluído. Foi mais forte lá porque as pessoas acreditaram na possibilidade de continuar a evoluir. Elas esperaram e demandaram.

O conceito de "esperanças crescentes" também explica o porquê de revoltas sociais frequentemente surgirem em locais de oportunidade em vez de em locais de opressão. A revolução flui a partir dos estudantes privilegiados das universidades, por exemplo. Líderes revolucionários notoriamente vêm das classes média ou alta, vêm da intelligentsia, e eles não partilham da vitimidade dos realmente oprimidos que alegam representar. De fato, os oprimidos frequentemente recusam trabalhar pela mudança social. Marx referiu-se a essa categoria da sociedade como o "lumpemproletariado" – o proletariado especificado pelos criminosos, vagabundos e os desempregados, que careciam de consciência [de classe] – ele os escarneceu por não entenderem ou não se importarem com o interesse de sua própria classe. Em vez de esperar por mudança, talvez eles estivessem fazendo o melhor que eles sabiam.

A maioria das revoluções terminam de forma ruim. Algumas começam de forma ruim, com violência e com uma erupção de raiva que parece visar mais a vingança do que a justiça. Até mesmo revoluções inicialmente pacíficas tendem a se dissolver em violência e terminam comandadas por líderes com agendas pessoais – sede de poder, ideologia, ganância, ou todos os fatores acima. Quando a fumaça cessa e os

cadáveres são removidos das ruas, o novo regime é louvado pela população. O novo regime rapidamente revela a si mesmo, entretanto, como sendo não menos tirânico que os tiranos que acabaram de serem destronados.

A Revolução Satoshi não corre esse risco. A blockchain é intrinsecamente pacífica, sem capacidade de cometer violência. A cripto não confronta os governos diretamente, decapita monarcas ou flamulam bastiões da opressão. Ela esquiva e torna-os obsoletos com eficiência brutal. Para aqueles embebidos na versão de revolução que só ergue barricadas, a asserção prévia pode parecer inofensiva. Mas, ao dar às pessoas liberdade financeira – até mesmo uma liberdade incompleta – a cripto é incendiária. O fluxo de trocas e de comércio produz a libertação porque produz a independência e a escolha. Ela estabelece uma revolução de esperanças crescentes que não é baseada em uma ideologia, mas no interesse próprio e racional das pessoas. Nada é mais poderoso.

Mas qual é a engrenagem que move a revolução Satoshi?

O Poder do Peer-to-Peer

O brilhantismo político da cripto reside em um fato: ela resolve o problema da "terceira parte confiável". (Aqui a palavra "confiável" significa o inverso de sua definição literal). Entender esse conceito é essencial para entender como funciona uma sociedade livre. Ainda assim, estava faltando para o léxico da liberdade.

Essa ausência causava estranheza. Depois de tudo, as principais dinâmicas do estado residem em forçar as pessoas a usarem as terceiras partes confiáveis da burocracia e das instituições associadas ao governo como um modo de as controlar. Se as pessoas desejam conduzir a vida cotidiana, elas não têm escolha senão fazer o acordo com as agências monopolistas do estado, incluindo reguladores, agentes de tributação, bancos centrais e impositores da lei. Terceiros confiáveis são o braço de ferro do estado. E é aí onde a parte "problema" do conceito surge. A camada intermediária entre o estado e o povo – a camada das terceiras partes confiáveis – é onde a corrupção e o controle germinam. Ao ordenar o uso dessas partes, o estado consolida sua autoridade e explora a pessoa comum. Sem que a população use suas terceiras partes confiáveis, o estado não tem meios de imposição. A ausência desse conceito é a chave para a ciência política.

A sociedade moderna parece exigir terceiras partes confiáveis, especialmente o sistema bancário central. De outro modo, é argumentado, seres humanos irão retornar às trocas diretas do escambo os quais são desorganizadas e muito limitadas no alcance geográfico do comércio e na variedade de bens trocados.

A cripto e a blockchain conseguiram virar o jogo. O whitepaper original de Satoshi, “Bitcoin: A Peer-to-Peer Cash System” (Outubro de 2008), explica, “O que é necessário é um sistema de pagamento eletrônico baseado em uma prova criptográfica em vez de em confiança, permitindo a quaisquer duas partes querendo transacionar diretamente uma com a outra o façam sem a necessidade de uma terceira parte confiável”. Essa é a raison d'être do Bitcoin.

Trata-se de uma questão de perspectiva, entretanto. Há uma função adequada – uma função de livre mercado – para terceiras partes confiáveis. É para facilitar as transações de indivíduos ao providenciar serviços, tais como a verificação de identidade providenciada por um notário. Tais terceiras partes confiáveis são subordinados ao livre mercado ao qual eles existem para servir. Mas até mesmo as terceiras partes confiáveis do livre mercado apresentam problemas. Um é inerente. A palavra “confiado” implica que não é sempre possível verificar se o terceiro é recorrível. Se a verificação fosse possível, então a necessidade de se confiar sequer iria aparecer como um problema; o termo seria “terceira parte verificada”. O risco surge em acordos privados, bem como em acordos públicos ou servientes ao estado. Por acaso um advogado opera clandestinamente em nome de si mesmo em vez de em nome de seus clientes, por exemplo? Confiar sua riqueza a outra pessoa é um negócio arriscado, mesmo se você conhecer bem a pessoa. Quando o terceiro é uma instituição impessoal sem contabilidade legal e paga pelo estado, tais como a imposição da lei, o risco aumenta astronomicamente.

Todas as instituições funcionam de acordo com seu próprio interesse e preservação. No livre mercado, o interesse próprio de um negócio é servir a seus clientes para lucrar e evitar perdê-los para seus competidores. Esse é um poderoso incentivo para estabelecer uma sólida reputação e manter a clientela satisfeita. O governo e suas terceiras partes monopolistas não possuem incentivo similar ou restrição porque as pessoas precisam lidar com elas. O estado regula todos os aspectos do mundo financeiro, por exemplo, o que força todos aqueles que desejam bancar ou negociar a interagir com instituições reguladas pelo estado.

Não há competição para a qual os monopólios possam perder clientes, e os monopólios que atendem necessidades humanas básicas nunca irão carecer de enchentes de clientela coagida. Se alguém precisa de uma conta bancária ou de um cartão de crédito para funcionar, então ele precisa aceitar quaisquer termos de serviço que o sistema bancário requer. Não há dúvida que esses termos beneficiam o banco e não o consumidor.

Aqueles que trabalham para terceiros estatistas não são necessariamente pessoas más, mas suas intenções e caráter não importam para o resultado. Burocratas, serventes civis, e banqueiros podem verdadeiramente acreditar que sua obra promove o bem público. Eles podem estar bem sorridentes, estar conscientes no trabalho, e até serem prestativos àqueles que usam seus serviços. Mas, isso não influencia o conteúdo do que eles produzem, a saber: um monopólio mandatado, através do qual o estado controla a riqueza e o comportamento da sociedade. Um burocrata bem-intencionado é parecido com um homem que trabalha em uma fábrica de conservas de atum e anuncia um dia que ele quer fabricar doces em vez de peixe enlatado. Na medida em que ele segue as regras da fábrica e usa as máquinas, ele irá produzir latas de atum e não barras de chocolate. Suas intenções não importam porque é o maquinário e o protocolo da fábrica o que determina o produto. O mesmo é verdade para agências do estado. Um policial pode sinceramente anunciar sua intenção de proteger direitos individuais contra a agressão do estado, mas enquanto ele segue as regras e mecanismos da imposição da lei, o produto resultante irá violar direitos individuais e sustentar o estado. Esse é um ponto importante do porquê um ataque ao estado não deveria se tornar um ataque a seres humanos que poderiam se tornar colegas viajantes.

O dilema: o comércio moderno e as finanças internacionais requerem intermediários, tal como um sistema de bancos interconectados que transmite dinheiro por uma longa distância. Novamente, a necessidade das pessoas por comércio as deixa abertas para exploração e controle pelo estado que apropria riqueza e informação ao dominar os intermediários.

Satoshi elegantemente resolveu esse problema. A cripto permite que as pessoas transfiram riqueza em uma base peer-to-peer que não requer intermediário, nenhuma terceira parte confiável. As transferências não podem ser arbitrariamente revertidas ou alteradas, de modo que

as duas partes não precisam confiar ou conhecer um ao outro; as intenções são irrelevantes. O melhor aspecto do escambo é mantido – troca direta – enquanto os piores aspectos caem por água abaixo – barreiras geográficas e uma limitada diversidade de bens. Visto que pessoas podem manter suas próprias carteiras, a necessidade de recorrer a um estabelecimento de armazenamento ou agente de transferência é também eliminada. Cada usuário pode funcionar como um banqueiro de si mesmo com carteiras seguradas por chaves privadas que previnem olhos e dedos maliciosos.

As implicações para a liberdade individual são profundas.

A Necessidade de um Dinheiro Descentralizado

Para as pessoas comuns se elevarem para além do escambo e abraçar a prosperidade do comércio moderno, um meio de troca é necessário – isto é, uma moeda corrente é necessária.

Economistas escrutinizam as características que um meio de troca desejável possui, tais como a ampla aceitação, durabilidade e fungibilidade.

Mas um aspecto crucial de uma moeda sólida é frequentemente ignorado: quem controla ela? Quem emite a moeda e decide as regras pelas quais ela circula? Uma moeda é tão sólida quanto as regras dentro das quais ela joga. Nos fins extremos do continuum social, há duas possíveis respostas. A moeda corrente está sob controle centralizado de uma autoridade ou o sob o controle descentralizado de cada pessoa a usando. Em outras palavras, a moeda corrente ou expressa o poder do estado ou a liberdade do indivíduo.

Em uma sociedade primitiva, a questão do que constitui uma moeda corrente válida é determinada pelas pessoas que negociam; elas podem decidir que querem usar conchas do mar, por exemplo. Para um observador de fora, a dinâmica poderia se assemelhar a um consenso centralizado porque a maioria das pessoas iriam achar conveniente escolher a mesma moeda corrente e tolerar as mesmas regras evoluídas. A moeda corrente, na verdade, expressa descentralização porque todo indivíduo pode resgatar sua participação a qualquer tempo e oferecer outros meios de troca. Essa é a característica definidora da descentralização; o indivíduo livremente entrega ou retira seu consentimento.

É dito que a sociedade moderna precisa de centralização porque sua complexidade requer coordenação massiva. Sociedades avançadas,

argumenta-se, demandam que decisões sejam coordenadas por um governo que crie a moeda corrente, defina sua circulação e elimine a fraude. Desconsiderando a objeção moral contra um monopólio da moeda corrente – a saber, que é errado compelir indivíduos pacíficos a usar ou a fazer qualquer coisa – ao menos duas outras objeções existem. A primeira fora esboçada anteriormente. O governo e suas instituições aliadas agem em prol de seu próprio enriquecimento e preservação, não em prol do interesse dos indivíduos forçados a usarem seus "serviços".

A segunda objeção é utilitária. Em sua Aula Memorial do Nobel de 1974, "The Pretense of Knowledge", o economista liberal clássico Friedrich Hayek explica:

> O reconhecimento dos limites insuperáveis para esse conhecimento deve [...] ensinar ao estudante da sociedade uma lição de humildade a qual deveria protegê-lo de se tornar um cúmplice da batalha fatal do homem para controlar a sociedade – uma batalha que não apenas o fará um tirano sobre seus semelhantes, mas que pode muito bem fazê-lo o destruidor de uma civilização ao qual nenhum cérebro designou, mas sim que cresceu dos esforços livres de milhões de indivíduos.

Ninguém possui informação o suficiente sobre as bilhões de transações que acontecem a todo minuto para centralizar ou controlá-las. Mesmo se fosse possível fazer isso por um momento congelado no tempo, o que não é o caso, preferências humanas e suas circunstâncias são imprevisíveis e talvez mudassem no próximo momento. O que foi verdade ontem pode não ser verdade hoje. Em resumo, Hayek acreditou que a engenharia social aleijou, ao invés de ter criado, a sociedade, porque ela impôs ignorância e preveniu os indivíduos de agirem segundo seu próprio interesse. Uma sociedade saudável é o resultado da ação humana, mas não do desígnio humano.

Um argumento pela centralização imediatamente surge. Se todo indivíduo persegue seu próprio auto interesse, então o caos é dito ser o resultado inevitável, especialmente quando um empenho envolve muitos indivíduos. O oposto é verdadeiro. O filósofo inglês do século XIX Herbert Spencer argumenta persuasivamente contra a noção de que a ordem social foi manufaturada pela coordenação através da lei. Em vez

disso, ele acreditava que a ordem desabrocha naturalmente das "cooperações espontâneas do homem perseguindo seus interesses privados."

Spencer contrasta duas formas de ordem: fileiras de soldados marchando em tandem (sociedade militar) e ordem espontânea (sociedade industrial). A última pode assemelhar-se ao caos, mas é na verdade uma forma inigualável de coordenação. Considere uma grande loja de departamentos durante uma corrida de Natal ao shopping. Uma pessoa olhando de cima a cena de uma perspectiva semelhante a divina veria as pessoas correndo em diferentes direções, às vezes esbarrando umas nas outras ou parecendo perdidas. Vendedores pegam itens do estoque apenas para colocá-los no chão de novo antes de se dispararem em diferentes direções. Eles desdobram roupas apenas para deixá-las em uma pilha bamba. O anúncio de uma promoção relâmpago faz com que elas entrem em uma debandada rumo à pechincha. Funcionários da loja correm de um lado para o outro para responder perguntas ou para dar desconto às pessoas. A cena pareceria "anarquista" no sentido caótico da palavra.

O que o observador vê, entretanto, é uma sofisticada versão da ordem espontânea pela qual todas as partes pacificamente atingem seus próprios caminhos sem coordenação centralizada. É um microcosmo do livre mercado em funcionamento. A loja quer vender seus bens, os empregados querem manter seus trabalhos, os clientes querem presentes. O que parece ser uma correria de várias formigas é o comportamento consciente e orientado a fins de indivíduos que não-intencionalmente beneficiam uns aos outros enquanto satisfazem suas próprias necessidades. Sem compradores no Natal, a loja pode ir à falência, os balconistas perderiam seus empregos; os vendedores não teriam pacotes embaixo da árvore de Natal. O caos aparente é o livre mercado trabalhando para satisfazer as necessidades das pessoas sem planejamento central, sem coordenação. E todos estão satisfeitos.

A Dinâmica da Cripto é similar. Sua descentralização de livre mercado depende de um consenso a partir do qual todos são livres para retirar seu consentimento sem punição. Os participantes não requerem conhecimento de transações além da deles mesmos, e eles chegam na blockchain de todas as direções para diferentes propósitos. O que parece caos é na verdade uma sofisticada forma de ordem que beneficia a todos.

O Primado da Privacidade

A privacidade da cripto é imperfeita, embora melhorias tecnológicas estejam sendo feitas. Ela providencia pseudonimato – um estado de identidade discreta que permite a confirmação de um usuário sem revelar sua identidade legal. Ademais, a cripto oferece uma forte camada de proteção contra abusos do estado e outras ameaças que surgem de olhos intrusivos. Instrumentos como os mixers podem, além disso, aumentar a proteção das criptos da identidade das pessoas, de seu Nome Verdadeiro. (Mais será dito sobre esse conceito.)

Privacidade e liberdade estão intimamente ligadas. Imagine um mundo onde a renda não é registrada. Como iriam os impostos ser coletados ou contas de banco confiscadas quando o governo não sabe o que você tem ou onde você tem? Se o registro de eventos de vida como o nascimento ou o ingresso na escola são privados, como poderiam nossas crianças serem recrutadas? Se a permissão não é requerida para abrir um negócio, como poderiam as regulações serem impostas? O maquinário do governo é paralisado sem a informação sobre quem você é e o que você tem. É por isso que seu apetite por dados é voraz. Conhecimento é poder. (Nota: as palavras “governo” e “o estado” estão sendo usadas intercambiavelmente).

Emprego, finanças, histórico médico, elegibilidade militar, educação, residência, estado conjugal, registro de telefone, hábitos de viagem, uso de internet, propriedade de automóveis e uma miríade de outros dados são ou armazenados pelo governo ou facilmente acessados por ele. A cripto providencia um raro oásis de privacidade baseado em algoritmos e pseudonimato. Quando a carteira de alguém envia um pagamento a outra, a chave daquele que enviou é decodificada pela chave de quem recebeu. A encriptação protege a transação de intromissão ou roubo. Sua privacidade protege a vida das pessoas do estado.

Essa é a visão de Satoshi Nakamoto: um sistema de comércio peer-to-peer, descentralizado e pseudonímico de comércio e de serviços bancários próprios através do qual o indivíduo evita a corrupção do atual sistema ao evitar utilizar terceiras partes confiáveis. Indivíduos privatizam as suas próprias vidas. Depois da prensa de Gutemberg, poucas invenções criaram tanta libertação e oportunidades para a liberdade.

Isso permanecerá verdade, entretanto, apenas se a visão original for sustentada e não comprometida por aqueles que perseguem “respeitabilidade” e equalizam essa palavra com sanção do estado.

Conclusão

A introdução focou na contribuição das criptos para o poder e para a liberdade dos indivíduos, mas o benefício da cripto para a sociedade civil é imenso.

Talvez nenhum outro autor tenha sido melhor em capturar os benéficos do auto interesse descoordenado da sociedade do que o filósofo do Iluminismo Francês François-Marie Arouet de Voltaire.

Em suas *Cartas a respeito da Nação Inglesa*, Voltaire pergunta o porquê de haver tanta tolerância religiosa na Inglaterra em comparação com a França, a qual foi despedaçada por conflitos brutais entre católicos e protestantes. Não foi devido a leis ou a história. As leis britânicas favoreciam fortemente a Igreja da Inglaterra e a perseguição passada foi severa o suficiente para fazer com que os Peregrinos fizessem uma perigosa viagem para um Novo Mundo. A diferença chave entre a Inglaterra e a França, conclui Voltaire, era a rede de comércio relativamente livre pela qual as pessoas comuns lidam umas com as outras somente por auto interesse financeiro. A diferença foi o surgimento de uma classe média comercial que rendeu para a Inglaterra o apelido de "uma nação de vendedores". A liberdade financeira alimentou a tolerância e a civilidade da sociedade.

Voltaire declara:

> Vá para a Bolsa de Londres, aquele lugar mais venerável que muitos tribunais, e você verá representantes de todas as nações reunidos lá em prol do lucro da humanidade. Lá o judeu, o maometano e o cristão lidam um com o outro como se fossem da mesma religião e reservam o nome de infiel para aqueles que vão a falência. Lá o presbiteriano confia no anabatista, e o anglicano aceita a promessa do quaker. Ao sair dessas reuniões pacíficas e livres, alguns vão à sinagoga, outros em busca de bebida; outro homem está a caminho de ser batizado em uma grande banheira em nome do Pai, pelo Filho, ao Espírito Santo; aquele homem está vendo o prepúcio de seu filho ser cortado, e uma fórmula hebraica será murmurada sobre a criança da qual ele mesmo não entende nada; alguns outros estão indo para sua igreja

esperar a inspiração de Deus com seus chapéus; e todos estão satisfeitos.

Ao permitir o livre fluxo de comércio e de riqueza, a cripto enriquece não apenas os indivíduos, mas também a sociedade civil, porque a interação financeira é a base da tolerância. Ela quebra barreiras raciais, étnicas e de classe. Bem como uma sociedade de encorajamento saudável, a cripto oferece diversidade de escolha para o indivíduo. Alguns usuários irão escolher o anonimato, enquanto outros podem divulgar suas identidades. Alguns irão ser individualistas severos e anarcocapitalistas, enquanto outros podem preferir o socialismo. Diferenças de ideologia, religião ou estilo de vida são irrelevantes para as transações em blockchain porque elas são cegas a tais delicadezas. Elas reconhecem apenas o consenso.

Uma sociedade em prosperidade é uma na qual as pessoas se reúnem em prol de seu próprio lucro, seja o lucro definido em termos monetários ou em termos culturais. Eles se reúnem em independência e liberdade. Eles separam seus caminhos quando querem seguir em frente. E todos estão satisfeitos.

SEÇÃO UM

O Problema da Terceira Parte Confiável

CAPÍTULO UM

Ouvindo o Passado

> "O problema chave com as moedas correntes convencionais é toda a confiança exigida para fazê-la funcionar. O banco central precisa ser confiado para que não venha a degradar a moeda corrente, mas a história das moedas fiduciárias está cheia de violações dessa confiança. Os bancos devem ser confiados para manter o nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito mesmo que mal tenham uma fração de reserva. Temos de confiar a eles a nossa privacidade, confiar neles para que não deixem ladrões de identidade drenarem nossas contas."
> – Satoshi Nakamoto

O problema das terceiras partes confiáveis têm assombrado os sistemas financeiros modernos e corretoras centralizadas porque as pessoas requerem um intermediário para fazê-las funcionar. Os bons ou maus motivos da terceira parte se tornam um aspecto definidor da transação, e aqueles que usam as instituições estão à mercê dessas intenções. Isso é especialmente verdade para o atual sistema de moeda emitida pelo estado e para o sistema bancário central.

Um sistema sem necessidade de confiança evita intermediários e não depende das intenções dos participantes; isto é, o sistema funciona da mesma maneira independente da intenção de qualquer parte. A blockchain, com um protocolo peer-to-peer imutável e transparente, é chamada de isenta da necessidade de confiança, porque não há intermediário corruptível do qual as trocas precisam depender.

Em uma pequena escala, o problema das terceiras partes confiáveis precisa sempre existir porque um intermediário é útil ou necessário em algumas situações. Se terceiras partes confiáveis oferecem serviços competitivos num livre mercado, entretanto, o dano da desonestidade ou incompetência é limitado. As pessoas podem levar seus negócios a todos os lugares, reportar um vigarista aos guardas, advertir aos outros e mover uma ação judicial.

Um terceiro ocasionalmente desonesto não é o problema, Satoshi adverte. Ele fala sobre a corrupção institucionalizada do governo e dos

bancos centrais a partir dos quais a pessoa comum não poderia escapar usando um competidor ou por processo judicial. Quase todos que trabalham numa mesa, dirigem um negócio, compram ou vendem bens, aceitam benefícios do governo ou pagam impostos tiveram de aceitar uma moeda fiduciária que constantemente afunda em termos de valor devido à inflação. Quase todos que usam crédito, aceitam cheques, tomam empréstimos, conduzem comércio ou fazem negócios no exterior precisam passar por bancos que roubam como assaltantes bêbados.

Para as pessoas comuns, a situação costumava parecer desesperançosa porque nenhuma alternativa legal, prática e privada existia para transferir fundos por consideráveis distâncias, incluindo fronteiras. Tentativas de reformar ou remover o sistema também pareciam condenadas porque elas eram inerentemente corruptas e auto servientes. De fato, o serviço bancário central e a moeda fiduciária estavam servindo ao propósito para o qual eles foram estabelecidos: controle financeiro pelas elites. A necessidade das pessoas por dinheiro e trocas se tornaram suas camisas de força.

E então veio Satoshi. E então vieram a blockchain e a cripto. Um novo conceito de dinheiro foi criado de uma forma que não pode ser inflacionada; o número de bitcoins é fixo em 21 milhões de unidades divisíveis. A oferta pode apenas diminuir quando moedas são perdidas, como inevitavelmente ocorre. Satoshi nota, “Moedas perdidas apenas fazem as moedas de todos os outros valerem um pouco mais. Pense nisso como se fosse uma doação a todos.” O Bitcoin resolveu o problema da moeda fiduciária.

Um novo conceito de transferência financeira resolveu o problema das terceiras partes confiáveis, especialmente no que diz respeito aos bancos. Embora transações peer-to-peer envolvam um intermediário ou minerador, nenhuma confiança é requerida visto que a transação é lançada apenas quando a “proof of work” é feita, o que consiste em resolver um complicado problema matemático. Chegar numa solução pode ser custoso do ponto de vista do poder computacional e gasto de tempo, mas as soluções em si mesmas são fáceis de verificar. Satoshi comenta, “Com uma moeda eletrônica baseada em prova criptográfica, sem a necessidade de se confiar numa terceira parte intermediária, o dinheiro pode se tornar seguro e as transações tornadas fáceis.” A solidez e propriedade do protocolo da blockchain é assegurada pelo uso de opensource que é visível a todos e por todos verificável. O resultado

político: Uma moeda corrente privada e um método de troca que libertou as pessoas da opressão financeira.

A própria ideia de uma moeda privada é, entretanto, dificilmente nova.

Precedentes na Teoria Individualista Radical

O velho Friedrich Hayek é o economista austríaco mais respeitado do século XX. Seu livro *The Denationalisation of Money: An Analysis of the Theory and Practice of Concurrent Currencies* argumenta vigorosamente a favor de moedas correntes privadas e competitivas, para que substituam as moedas emitidas pelo governo. Hayek pondera uma questão chave. “Quando se estuda a história da moeda não será de ajuda perguntar o porquê de as pessoas terem persistido com governantes exercendo um poder exclusivo por mais de dois mil anos que foram regularmente usados para explorar e defraudá-las. Isso pode ser explicado somente pelo mito” de que a moeda do governo precisava “tornar-se tão firmemente estabelecida que não passou pela cabeça dos estudantes profissionais dessas áreas […] sequer questionar isso. Mas uma vez que a validade da doutrina é questionada, seu fundamento é rapidamente percebido como frágil.”

Os governos arrancam lucros incríveis ao degradar a moeda, mas o jogo manipulado funciona apenas se as pessoas não têm alternativa senão jogá-lo. O propósito político das leis bancárias e de curso forçado é garantir um monopólio ao estado, que permitem a redistribuição de riqueza e de poder das pessoas comuns para além da elite da sociedade. A moeda fiduciária e os sistemas bancários, entretanto, permanecem frágeis, porque o sistema depende de pessoas que ou não entendem as dinâmicas, ou que entendem e não tem escolha. Hayek se pergunta o porquê de o entendimento público ser tão enganoso. Pois havia “um monopólio do governo da provisão de dinheiro […] universalmente tido como indispensável” e o que iria acontecer “se a provisão do dinheiro fosse aberta para a competição de preocupações privadas ofertando diferentes moedas correntes?”

Com estranha presciência, Hayek argumenta a favor de moedas correntes desenvolvidas por empreendedores que inovam em novas formas de dinheiro assim como eles inovam em outras áreas. Uma das desvantagens do monopólio do governo é que ele impõe um congelamento do tipo de invenções que agora correm livres nas criptos. O historiador

voluntarista Carl Watner observa: “Ninguém pode falar em antecipação quais as formas de moedas que podem surgir porque ninguém tem certeza de que escolhas os indivíduos fariam ou que novas tecnologias podem ser descobertas. Leis forçando as pessoas a usarem o dinheiro do Federal Reserve System congelaram os desenvolvimentos monetários em um certo estágio. […] Imagine se o Congresso tivesse protegido os Correios ao aprovar leis que iriam ter prevenido as pessoas de se comunicar via internet. Nós nunca iríamos ter experienciado as maravilhas do e-mail.”

O tardio economista austríaco Murray Rothbard também disputa a questão de “por que as pessoas resistem tão vigorosamente a moedas privadas?” Em seu livro *For a New Liberty: The Libertarian Manifesto* ele antecipa uma explicação." Se o governo e apenas o governo tivesse tido um monopólio da manufatura de sapatos e dos negócios de varejo, como iria a maior parte do público tratar o libertário que veio agora defender que o governo saia do negócio de sapatos e que o mercado seja aberto para os empreendimentos privados?". Rothbard prevê que os céticos iriam atacar o libertário por privá-lo da única fonte possível de sapatos – o governo. As pessoas são completamente doutrinadas a acreditar que a vida cotidiana não pode funcionar sem o estado e a moeda fiduciária.

Hayek e Rothbard são incomuns entre os economistas do livre mercado no que diz respeito a sua adoção ao dinheiro e a sistemas monetários privados. Até mesmo os zelotes do laissez-faire raramente defendem moedas de livre mercado ou serviços bancários privados. Em vez disso, eles debatem questões marginais tais como reserva fracionária e outras reformas que eles acham que irão melhorar o sistema existente. Ou eles argumentam pela restauração de um padrão ouro como se isso fosse uma panaceia. Mas, se um padrão ouro fosse aplicado à moeda fiduciária, o sistema ainda iria exigir que as pessoas confiassem no governo e nos bancos. Isso significa confiar que ambas as instituições iriam agir contra os seus próprios interesses, os quais eles historicamente negligenciaram-se a fazer.

A negligência moderna do dinheiro e dos serviços bancários de livre mercado é estranha porque os individualistas do século XIX focaram intensamente na importância da moeda privada e dos serviços bancários privados para a libertação pessoal. Eles colocaram uma ênfase primária no direito de todo indivíduo criar a sua própria moeda e funcionar como o seu próprio banco. Era um direito natural tão importante

quanto a liberdade de fala ou religião. O proeminente individualista Benjamin Tucker acreditou que o direito de usar a moeda privada era tão importante que esse direito poderia destruir o Estado totalmente por si mesmo. Seu raciocínio: o monopólio monetário, incluindo o controle do crédito, foi como o Estado sustentou a si mesmo e roubou as pessoas comuns não apenas de riqueza, mas também de oportunidades econômicas.

Dois eventos específicos esculpiram a abordagem que os primeiros anarquistas individualistas adotaram em relação ao monopólio monetário. Um deles foi o *Pânico de 1837*, que levou os Estados Unidos à recessão até meados da década de 1840. As causas comumente citadas do Pânico incluem uma bolha imobiliária em colapso e uma queda acentuada nos preços do algodão. A culpa também é colocada nos pés do presidente Andrew Jackson por vetar a recuperação do Segundo Banco dos Estados Unidos e precipitar uma infeliz cadeia de eventos econômicos. Baseando-se no trabalho do professor de economia Peter Temin, Rothbard contesta essa interpretação.

> Primeiro, ele [Temin] aponta que a inflação de preços realmente começou mais cedo, quando os preços em geral atingiram um mínimo de 82% em julho de 1830 e depois subiram em 20,7% em três anos para chegar a 99% no outono de 1833. A razão para o aumento de preço é simples: A oferta total de dinheiro havia aumentado de $109 milhões em 1830 para $159 milhões em 1833, um aumento de 45,9%, ou um aumento anual de 15,3%. Dividindo ainda mais os números, a oferta total de dinheiro aumentou de $109 milhões em 1830 para $155 milhões um ano e meio depois, uma expansão espetacular de 35%. Inquestionavelmente, essa expansão monetária foi estimulada pelo ainda florescente Banco dos Estados Unidos, que aumentou suas notas e depósitos de janeiro de 1830 a janeiro de 1832 de um total de $29 milhões para $42,1 milhões, um aumento de 45,2%. Assim, a inflação de preços e dinheiro nos primeiros anos da década de 1830 foi novamente desencadeada pela expansão do ainda dominante banco central.

Pode-se dizer que o Pânico começou em maio de 1837, quando os bancos da cidade de Nova York anunciaram que não iriam resgatar

papel comercial em espécie pelo valor de face integral. Dos aproximadamente 800 bancos nos Estados Unidos, todos, exceto seis, pararam em um ponto ou outro de resgatar notas e depósitos por moedas de ouro ou prata. A suspeita e o ódio aos bancos tradicionais e ao dinheiro emitido pelo governo dispararam, com radicais examinando sistemas alternativos.

O outro evento que impactou dramaticamente a febre radical da reforma monetária foi a Guerra Civil, pela qual o Norte financiou sua luta por meio de Leis de Curso Legal e do National Banking Act de 1863.

Os radicais não apenas teorizaram; eles experimentaram moedas privadas e novos modelos econômicos. Seus esforços são fascinantes, mas também são histórias de advertência. Um grande problema para o anarquismo individualista do século XIX foi a aceitação geral do movimento de que havia um elo entre dinheiro sólido e a teoria do valor-trabalho. Esta teoria afirma que o verdadeiro valor de um bem ou serviço é baseado no trabalho necessário para produzi-lo, e não no preço pelo qual um vendedor e um comprador estão dispostos a trocar. Em suma, um bem tem valor intrínseco e não subjetivo. (Mais sobre isso na seção sobre o Teorema da Regressão). Felizmente, seu principal objetivo econômico era a abolição do “monopólio do dinheiro”. O termo se referia a três formas diferentes, mas interativas de monopólio: bancos, cobrança de juros e emissão privilegiada de moeda. A abolição do poder estatal sobre a moeda era o foco, e eles evitavam o uso da força para implementar seus próprios esquemas.

Josiah Warren forneceu um exemplo real do que se entende por moeda baseada na teoria do valor-trabalho. Creditado como o primeiro anarquista americano, Warren testou sua solução específica para o monopólio do dinheiro através de uma Loja de Tempo da qual ele emitiu “Notas de Trabalho”. Em 1827, a empresa abriu com $300 em mantimentos e produtos secos que foram oferecidos com uma margem de 7% dos custos de Warren para cobrir despesas de administração. Isso foi antes de os mantimentos serem pré-embalados ou pré-pesados, e era comum que os compradores negociassem com o lojista em vez de pagar um preço postado. Uma das inovações de Warren foi colocar preços, o que reduziu os custos porque as transações consumiam menos tempo. O cliente pagou em dinheiro tradicional pelas mercadorias e pagou com uma Nota de Trabalho para compensar Warren por seu tempo. A Nota de Trabalho obrigava o cliente a fornecer a Warren uma quantidade

equivalente de seu tempo. Se a compradora fosse uma costureira, por exemplo, a Nota de Trabalho a obrigava a render a Warren X unidades de tempo para produzir roupas. O objetivo de Warren era estabelecer uma economia – ou pelo menos estabelecer uma prova de princípio – na qual o lucro fosse baseado na troca de tempo e trabalho. As Notas de Trabalho circularam e foram amplamente negociadas na comunidade.

Até certo ponto, Warren teve sucesso. As pessoas viajavam centenas de quilômetros de distância para aproveitar os preços baixos da Loja de Tempo. Depois de alguns anos, ele declarou o experimento um sucesso e fechou a loja. Que as Notas de Trabalho tenham sido um sucesso é questionável, no entanto. A própria loja pode ter tido sucesso devido aos seus preços baixos, não às Notas. Qualquer que seja a explicação verdadeira, é difícil ver como essa nova moeda poderia funcionar em populações densas ou em uma escala maior de comércio. Poucas pessoas hoje estariam convencidas da viabilidade do dinheiro privado com base no experimento da Loja de Tempo.

O que será que convenceria o público e os economistas de que as moedas privadas funcionam tão bem ou melhor do que as emitidas pelo governo? Voltar um pouco mais longe na história americana é um bom ponto de partida, porque o futuro sempre se sustenta no passado.

A América nasceu na moeda privada

A América colonial ensina lições poderosas sobre moedas privadas.

As colônias britânicas naturalmente usavam moeda britânica, mas as políticas monetárias duvidosas da pátria também criaram um apetite voraz por dinheiro alternativo. Rothbard explica em *A History of Money and Banking in the United States: The Colonial Era to World War II*, “A Grã-Bretanha estava oficialmente em um padrão de prata […] No entanto, a Grã-Bretanha também cunhou ouro e manteve um padrão bimetálico. […] Na Grã-Bretanha dos séculos XVII e XVIII, o governo manteve uma razão de cunhagem entre ouro e prata que consistentemente supervalorizou o ouro e subvalorizou a prata em relação aos preços do mercado mundial.” As políticas da Grã-Bretanha criaram um mercado robusto de substitutos para seu próprio dinheiro.

A Lei de Gresham governava o dinheiro colonial da mesma forma que governa todas as moedas. A Lei: se duas moedas forem oficialmente avaliadas pelo mesmo preço ou por uma proporção fixa e o valor

de mercado de uma for maior, então a moeda mais valiosa desaparecerá da circulação geral e será usada de outra maneira, como a acumulação de poupança ou pagamento de dívidas externas. Este é o significado do axioma “a moeda ruim expulsa a boa”. Moedas de prata encorpadas começaram a desaparecer da circulação dentro das colônias, se transformaram em prata mais leve, dinheiro baseado em mercadorias ou moedas estrangeiras e cunhadas de forma privada. Essas moedas funcionavam como moedas totalmente paralelas, com os peso de ocho espanhóis sendo particularmente populares.

A primeira moeda americana cunhada em particular parece ser o Granby ou Higley Token, que foi cunhado por Dr. Samuel Higley de Connecticut em 1737. Após a morte de Samuel, seu irmão John produziu as moedas de cobre de 1737 a 1739 inclusive. Avaliando as fichas em três pence cada, John supostamente gastou a maioria delas no bar local, até que o barman se recusou a aceitar mais. Em seguida, ele lançou moedas com um lado dizendo “Valore-me como quiser” e o outro lado declarando “Eu sou bom cobre”. Nenhum valor foi estampado na moeda, o que era prática comum naqueles dias. Eles circularam amplamente por muitos anos, mesmo depois que John deixou de os cunhar, porque eram uma liga confiável com a qual os ourives faziam joias. Análises metalúrgicas posteriores do Granby descobriram que as moedas eram 98-99% de cobre puro.

Outra lição: o ourives de Nova York do século XVIII, Ephraim Brasher, demonstrou um método pelo qual as moedas cunhadas em particular podiam circular amplamente e sem dúvidas sobre sua pureza ou peso. Muitos cunhadores privados tinham boa reputação dentro de suas próprias comunidades, mas a circulação de suas moedas era frequentemente limitada a esses arredores. Brasher ofereceu uma solução. Ele tornou-se conhecido por testar moedas nas quais carimbava “EB” se provassem ser seguras. Apoiadas por sua reputação, as moedas carimbadas migraram por toda parte.

Esta é uma grande vantagem que a cripto tem sobre as moedas privadas anteriores; suas moedas não têm a mesma necessidade de serem lastreadas por verificação. Ao contrário das moedas físicas, as bitcoins não podem ser raspadas, falsificadas, diluídas por ligas ou negadas pelos maus atos dos mineradores ou dos usuários. Um bitcoin é um bitcoin, e ninguém pode alterar esse fato. Isso evita a verificação de pureza ou peso.

Como e por que o governo proibiu o dinheiro privado

Como a ratificação da Constituição dos Estados Unidos em 1788 afetou o dinheiro privado?

Pessoas assumem que a Constituição dos Estados Unidos concede ao Congresso um "direito" de monopólio de emitir dinheiro. A suposição vem do artigo 1º, Seção 8, Cláusula 5 da Constituição que delega ao Congresso o poder de "cunhar moeda, regular seu valor, e de moeda estrangeira, e fixar o padrão de pesos e medidas". Este é considerado um direito de monopólio. Em seu panfleto "A Inconstitucionalidade das Leis do Congresso Proibindo Correios Particulares" (1844), o jurista e defensor do dinheiro privado Lysander Spooner explica o contrário:

> [Os] poderes do Congresso [...] para "cunhar dinheiro" são na realidade exclusivos apenas contra os governos de outros estados. [...] A proibição constitucional sobre os indivíduos de cunhar dinheiro não se estende além das proibições de "falsificar os títulos e moedas atuais dos Estados Unidos". Desde que os indivíduos não "falsifiquem" ou imitem "os títulos ou moedas correntes dos Estados Unidos", eles têm todo o direito, e o Congresso não tem poder para proibi-los de pesar e analisar peças de ouro e prata, marcar neles seus pesos e pureza e vendê-los pelo que eles trouxerem em competição com a moeda dos Estados Unidos.

A Constituição trata da regulamentação da "moeda estrangeira", mas as moedas domésticas privadas permaneceram populares, especialmente uma chamada de Bechtler.

O século XIX viu uma onda de corridas de ouro na América do Norte. No final da década de 1820, tanto a Geórgia quanto a Carolina do Norte experimentaram grandes corridas e um dilema que as acompanhava. Não havia cunhagem governamental na área. O envio de ouro para a principal casa da moeda na Filadélfia era problemático, porque custava muito para transportar e segurar. Um jornal local explicou a situação da mineradora:

> Já que o Banco do Estado limitou suas emissões e está recolhendo em seus cofres as notas que foram emprestadas

> aos nossos cidadãos, na liquidação de suas contas pendentes, grande inconveniência tem sido deixada em transações comerciais com o Banco, e para fins comuns de comércio. Até que ponto esse esquema [ter uma casa da moeda privada] conseguirá concretizar esses objetos, ainda temos que aprender. O risco e a despesa de enviar ouro para a casa da moeda [Filadélfia] é tal que os proprietários das minas muitas vezes acham difícil descartar os produtos das minas a um valor justo, como as coisas estão agora. Tendo falhado a petição urgente ao Congresso para o estabelecimento de uma filial da Casa da Moeda dos EUA na “região do ouro”, e o ouro produzido estando em condições justas de desaparecer completamente do país e cair nos tesouros enferrujados da Europa, esse esquema foi utilizado.

Os garimpeiros procuraram o respeitado relojoeiro e ourives Sr. Christopher Bechtler para uma solução particular. Por ser também metalúrgico e homem honesto, Bechtler era o candidato perfeito para começar a cunhar moedas. A primeira moeda de ouro Bechtler emitida em 1831 foi seguida de anúncios declarando que Bechtler cunharia o ouro de qualquer minerador por 2,5% do ouro.

A reação do governo à competição pode ser julgada pelo fato de que o Tesouro dos Estados Unidos perdeu pouco tempo testando as novas moedas, provavelmente na esperança de desacreditá-las. Infelizmente para o Tesouro, os Bechtlers eram mais puros do que as emissões governamentais. De fato, a Casa da Moeda Federal comprou $294.000 em Bechtlers e os usou para pagar dívidas e negociar com a Europa. De repente, o governo foi motivado a abrir sua própria casa da moeda federal em Charlotte, Carolina do Norte, que ficava a cerca de 130 quilômetros da de Bechtler. A Casa da Moeda Federal começou a produzir moedas de ouro em 1838.

Na época da morte do Sr. Bechtler, consideravelmente mais de um milhão de Bechtlers circulavam amplamente na América, particularmente no Sudeste. A partir daí, porém, os parentes que assumiram o negócio eram incompetentes ou desonestos. A consistência e a pureza diminuíram, e o mercado respondeu se afastando. A casa da moeda fechou alguns anos depois porque ela viveu e morreu de sua reputação.

Os Bechtlers originais continuaram a circular, no entanto. Eles eram tão populares que, durante a Guerra Civil Americana (1861-1865),

as obrigações monetárias da Confederação foram especificadas como sendo pagáveis em ouro Bechtler, não confederado ou outra moeda emitida pelo governo.

A moeda Bechtler é tanto um conto inspirador quanto um aviso. Ele fala das consequências de integridade e degradação do livre mercado, que não são problemas para a cripto porque são isentas da necessidade de confiança e as moedas não podem ser alteradas. A história de Bechtler também demonstra como o livre mercado supera o governo em termos de mover-se rapidamente para um nicho vazio e produzir qualidade. Como fazem hoje, as moedas de livre mercado superam as emissões governamentais. Se eles deixarem de fazê-lo, a moeda falha devido à Lei de Gresham. Como fez no passado, o governo hoje usa moedas privadas, como ouro e criptomoeda, enquanto tenta minar a concorrência que elas representam por meio de suas leis.

A resistência do governo à concorrência não começou nem terminou com os Bechtlers, é claro. Em seu ensaio "Hard Money in the Voluntaryist Tradition", Watner traça o curso de uma casa da moeda em São Francisco durante a corrida do ouro na Califórnia: Moffat & Co. "A Moffat & Co. foi aparentemente a mais responsável das empresas privadas de cunhagem de dinheiro", pois quando "os negócios de São Francisco colocaram um embargo em todas as cunhagens de moedas de ouro privadas", a exceção foi a Moffat. "O restante das emissões privadas foi logo enviado ao Gabinete de Ensaio dos EUA para ser derretido ou então foi aprovado apenas por seu conteúdo de ouro no comércio."

Inicialmente, a Moffat emitiu lingotes de ouro em concorrência direta com o Gabinete Federal de Ensaio dos EUA porque não existia então nenhum Gabinete de Ensaio do estado. De acordo com o site de referência *Coinfacts*, "o ensaio oficial do governo desses lingotes provou que eles valem mais do que o valor estampado neles". A Moffat superou o governo.

A denominação dos lingotes era muito grande para o comércio normal, no entanto, e os comerciantes exigiam moedas menores. A Moffat havia feito um acordo com o Gabinete de Ensaios dos EUA e agora pedia autoridade para cunhar moedas, bem como os lingotes maiores. Quando a permissão não veio, Moffat começou a cunhar moedas sob sua própria marca e autoridade em 1849. A alta reputação da firma e sua política de resgatar todas as moedas pelo valor nominal fizeram com que sua emissão se tornasse uma moeda circulante popular.

A obstrução do governo não parou com a recusa de autorizar a cunhagem. Em 20 de abril de 1850, o State Assayer, Melter, and Refiner of Gold of California foi estabelecido por lei. Um projeto de lei complementar foi aprovado ao mesmo tempo com o objetivo de frear os cunhadores privados. Junto com uma medida anterior em 8 de abril, o projeto representava um compromisso. *Coinfacts* explicava a posição original que o governo havia tomado em relação a cunhadores como Moffat.

> Foi durante a primeira metade de 1850 que houve uma séria agitação contra a cunhagem privada. O Legislativo da Califórnia considerou um projeto de lei [...] que teria rotulado cunhadores privados como falsificadores, e que insistia em sujeitar "os fabricantes ou passadores de tal moeda à penalidade imposta aos cunhadores e falsificadores". O projeto de lei também teria forçado as casas de moeda privadas a resgatar suas moedas em "dinheiro legal". A *Alta Califórnia* imprimiu o projeto de lei junto com um editorial de apoio. O editor apontou ainda a impossibilidade de usar moedas privadas no pagamento da alfândega.

No dia seguinte, a *Alta Califórnia* divulgou uma carta aberta da própria Moffat através da qual ela apelou ao povo de São Francisco. Ela reconheceu que o estado não podia emitir moedas legalmente devido a restrições constitucionais, mas os particulares não tinham restrições semelhantes. Ela apontou para a casa da moeda Bechtler que continuava a produzir moedas, embora o negócio estivesse a apenas 130 quilômetros da filial do governo federal em Charlotte. A Moffat lembrou poderosamente a São Francisco que ninguém jamais havia sido enganado comprando ou aceitando suas moedas.

A primeira lei de compromisso do início de abril proibia a emissão privada de peças de ouro com peso inferior a quatro onças troy. Mais uma vez, este era um tamanho estranho para o comércio normal e quase garantia uma circulação limitada. Por outro lado, o Departamento de Ensaios do estado foi autorizado a fundir lingotes de ouro de duas onças troy. *Coinfacts* observou: "O Escritório Estadual de Ensaios da Califórnia foi uma instituição única na história de nossa nação. Foi a única casa da moeda a operar neste país sob a autoridade de um estado,

depois de 1789. Suas emissões (embora nunca contestadas nos tribunais) podem ter sido ilegais sob a Constituição dos Estados Unidos, que proibia qualquer estado de emitir moedas metálicas ou moedas correntes”. O estado usou a artimanha de emitir lingotes que não foram mencionados na Constituição, mas que circulavam como o equivalente a moedas.

O projeto de lei de 20 de abril prejudicou ainda mais os cunhadores privados, exigindo que eles resgatassem suas moedas pelo valor nominal para emissão do governo. Seguiu-se uma complicada ida e volta entre a Moffat e os escritórios de análise estadual e federal. A Moffat recebeu um contrato de cunhagem com o estado e buscou permissão federal para cunhar moedas menores; foi negado. Eventualmente, Moffat voltou a emitir suas próprias moedas em denominações menores, após o governo ter concedido à empresa permissão para emitir moedas oficiais de $10 e $20 para o Gabinete de Ensaio.

O governo federal mudou de tática em 1852. A Alfândega dos EUA de repente se recusou a aceitar os lingotes de US $50 de Moffat, embora tivessem sido emitidos sob a autoridade direta do Gabinete de Ensaios dos EUA.O pagamento da alfândega era o principal uso dos lingotes, mas a lei federal exigia que os impostos fossem pagos em moedas com 900/1000 de pureza, em vez do padrão da Califórnia de 884/ a 887/1000. O Departamento do Tesouro deu o notável passo de se recusar a aceitar moedas emitidas por seu próprio Gabinete de Ensaios. Ela invalidou a sua própria cunhagem.

A história da Moffat & Co. é significativa não apenas porque ilustra como o dinheiro privado pode e irá atender às necessidades públicas, mas também porque revela a determinação absoluta do governo de eliminar a concorrência na moeda e as táticas que costumava usar. As táticas permanecem as mesmas até hoje. Uma é proibir a moeda criminalizando-a, como a legislatura da Califórnia tentou fazer com a acusação de falsificação. Outra é absorver e controlar a concorrência como fez o Gabinete de Ensaio ao contratar com a Moffat. Uma terceira estratégia é colocar enormes obstáculos no caminho das moedas livres, o que equivale a uma proibição de facto e dá uma vantagem decisiva ao dinheiro do governo.

A estratégia do governo funcionou. Watner explica: “Em outubro de 1856, a Casa da Moeda federal aparentemente foi capaz de atender a toda a demanda de moeda em circulação doméstica e para exportação, de modo que as emissões privadas de moedas de ouro desapareceram

silenciosamente. Não há registro de nenhuma outra cunhagem privada na Califórnia depois dessa época.”

A história da cunhagem privada no início da América é profunda, difundida e intimamente ligada ao sucesso econômico da nação. A fraude certamente estava presente, mas a honestidade meticulosa e as soluções para a fraude também. As casas da moeda com grande reputação e bom senso comercial tiveram sucesso, e muitas vezes superaram suas contrapartes governamentais, reduzindo-as ao uso da força (lei) para ganhar vantagem.

O governo não agiu em nome do público. Se tivesse, não teria atacado empresas honestas que prestavam serviços desesperadamente necessários a mineradores, comerciantes e compradores; a necessidade pública de moeda foi ignorada pelo Departamento do Tesouro. A lei também não explica por que alguns governos preferiram usar moedas privadas em algumas ocasiões. Uma explicação faz sentido; o governo queria eliminar a concorrência não porque fosse fraudulenta, mas porque a concorrência poderia vencer em um livre mercado. O governo agiu em seu próprio nome para encher seus bolsos e fortalecer seu poder.

Em 8 de junho de 1864, o Congresso aprovou uma lei para punir e impedir a falsificação de moedas dos Estados Unidos. Dizia, na íntegra:

> Que se qualquer pessoa ou pessoas, exceto as agora autorizadas por lei, fizerem ou fizerem ser feitas, ou emitirem ou passarem, ou tentarem emitir ou passar, quaisquer moedas de ouro ou prata, ou outros metais ou ligas de metal, destinados ao uso e finalidade de dinheiro corrente, seja na semelhança da moeda dos Estados Unidos ou de países estrangeiros, ou de desígnio original, toda pessoa que assim infringir deverá, mediante condenação, ser punido com multa não superior a três mil dólares, ou com prisão por um período não superior a cinco anos, ou ambos, a critério do tribunal, de acordo com o agravamento do delito.

A cunhagem privada de moeda efetivamente cessou na América.

A Lei foi, sem dúvida, vendida ao público como sendo necessária para proteger contra fraudes. Sem desculpar qualquer fraude existente

ou sugerir que o crime não deveria ser punido, uma política de advertência ou "comprador, cuidado" deveria ser aplicada; o comprador é responsável por verificar a qualidade das mercadorias antes de uma compra. Muita fraude poderia ter sido evitada se as pessoas não tivessem confiado nas garantias do governo, mas tivessem aprendido a avaliar a qualidade por si mesmas. Uma categoria inteira e valiosa de negócios foi criminalizada porque alguns participantes eram desonestos e alguns clientes descuidados. Essas foram as desculpas. A principal motivação para o governo foi eliminar a concorrência.

É reputada a Mark Twain a seguinte fala: "A história não se repete, mas rima". Para alguns, a cunhagem privada no início da América pode parecer ter pouco em comum com a cripto, mas há um tema comum. O governo está ameaçado e quer monopolizar ou regular um novo dinheiro privado através de uma mistura de proibição, levantamento de obstáculos, absorção e punição. A história está começando a rimar.

Em última análise, a viabilidade de criptomoedas e outras moedas privadas se resume a duas perguntas: O livre mercado pode fornecer um dinheiro competitivo? E o estado permitirá que o dinheiro privado exista sem regulamentação?

Um grande obstáculo para a aceitação da cripto nos círculos de livre mercado tem sido a convicção de que ela não é e não pode ser um dinheiro válido.

O Teorema da Regressão

O exemplo da moeda de Granby que continuou a circular devido ao seu valor na fabricação de joias ilustra um princípio que gerou debate sobre se a cripto pode ser vista como uma moeda. O conceito é o Teorema da Regressão.

O Teorema da Regressão é uma proposição econômica que está mais associada a Ludwig von Mises. Aplica a teoria subjetiva do valor ao poder de compra ou valor objetivo do dinheiro. O teorema faz isso traçando valores de troca objetivos através da "teoria subjetiva do valor, pela qual os valores são atribuídos aos valores de uso subjetivos finais dos consumidores marginais que valorizam tais bens e serviços por seus valores de uso objetivo que eles esperam consumir". Em outras palavras, o valor de uso objetivo do dinheiro remonta ao ponto em que as pessoas valoravam seus usos não monetários. Isso levanta um problema para a moeda fiduciária que não é consumida como o ouro ou a prata

podem ser. Em vez disso, com a moeda fiduciária, “os valores de uso subjetivo e objetivo do dinheiro coincidem e são iguais ao seu valor objetivo de troca, o valor estimado dos bens e serviços pelos quais ele pode ser trocado.”

O professor de Economia Jeffrey Rogers Hummel descompacta o conceito, revelando como se aplica à moeda fiduciária. O poder de compra do dinheiro de hoje “se baseia no de ontem, e no de ontem desse ontem… e assim em diante. […] Até quão longe a regressão […] vai? Logicamente, Mises explicou, para um dinheiro mercadoria ela vai até o dia em que a mercadoria pela primeira vez passou a ser usada como um meio de troca. Nesse dia, ele teve um valor de troca ou poder de compra devido apenas” a sua importância “como uma mercadoria comum (para consumo ou para uso como uma entrada produtiva) e não para uso como um meio de troca. Pois […] o dólar dos EUA se tornou uma moeda fiduciária ao terminar com a resgatabilidade do que fora uma reivindicação para um dinheiro mercadoria […]. A cadeia histórica regride para o dia antes da terminação, e, portanto, de volta ao dia antes da mercadoria se tornar um meio de troca. A aplicação da lógica para uma nova moeda fiduciária” significa aplicar uma taxa de resgate oficial para uma moeda fiduciária estabelecida.

O teorema tem sido muito influente porque ele elegantemente entrelaça o poder de compra do dinheiro com as teorias de valor subjetivo e de utilidade marginal. A teoria subjetiva do valor argumenta que nenhum bem ou serviço é inerentemente valioso; não tem valor embutido devido ao trabalho necessário para produzi-lo, por exemplo. Em vez disso, seu valor é determinado pela importância do bem ou serviço para os indivíduos específicos que o vendem e consomem. Mas esse valor não permanece constante mesmo para esses indivíduos por causa da utilidade marginal. A utilidade marginal refere-se à satisfação adicional que uma pessoa recebe ao consumir mais uma unidade de um bem ou serviço, medida em números ordinais. Um homem faminto provavelmente valorizaria um prato de comida como o 1° da lista, enquanto uma pessoa com excesso de peso em uma dieta rigorosa pode dar ao mesmo prato uma classificação negativa. Depois de comer o suficiente, o homem faminto provavelmente desvalorizará a utilidade marginal de mais comida e priorizará encontrar abrigo para a noite. Todo valor econômico é subjetivo e está em fluxo.

O Teorema da Regressão precisa ser cuidadosamente ponderado apenas porque muitos economistas austríacos e outros economistas de

livre mercado rejeitam a criptomoeda alegando que ela viola as circunstâncias nas quais o dinheiro válido deve se originar; essas pessoas deveriam ser aliadas naturais da comunidade cripto, não críticas. Enquanto isso, a maioria dos entusiastas de cripto reagem de uma das quatro maneiras ao ouvir a objeção do Teorema da Regressão. Elas não ligam. Assumem a atitude de "se cachorro come, é comida de cachorro"; ou seja, se algo compra bens e serviços, é dinheiro. Eles afirmam que o teorema não se aplica para a era digital. Ou eles insistem que se *aplica* à cripto de uma maneira que é mal compreendida. As duas últimas abordagens são promissoras para resolver o que parece ser uma tensão entre Mises e a cripto. Ambos os lados podem se beneficiar de clarificação.

Um ponto inicial: Um teorema é uma proposição geral que não é evidente em si mesma, mas precisa ser provada por uma cadeia de raciocínios. Tem sido chamado de "uma verdade estabelecida por meio de verdades aceitas". Não é um axioma e é vulnerável a mudanças nas circunstâncias ou no raciocínio adicional. Isso significa que a proposição é maleável.

O economista Robert P. Murphy fornece outro caminho para explicar como o Bitcoin surgiu como um meio de troca sem estar vinculado a uma mercadoria ou resgatável em um valor fixo de uma moeda fiduciária estabelecida. Seu artigo "Why Misesians Need to Tread Cautiously When Disparaging Bitcoin" argumenta: "[As] primeiras pessoas a negociar por ele o fizeram porque lhes fornecia utilidade direta, porque sabiam que havia pelo menos uma chance de servir para irritar os governos do mundo […] [Os] primeiros adeptos do Bitcoin estavam fazendo isso por razões ideológicas, não por razões pecuniárias". Para Murphy, a liberdade é o valor de mercadoria ou serviço do bitcoin.

O cripto-entusiasta Jeffrey A. Tucker usa uma tacada diferente. Em um artigo da *Foundation for Economic Education* intitulado "What Gave Bitcoin Its Value?", ele aponta para o propósito que o teorema serviu originalmente; ajudou a responder à pergunta de por que certas mercadorias surgiram como moedas enquanto outras não. O surgimento do sal como uma moeda, em vez de algas marinhas, foi devido à utilidade direta e durabilidade do sal, por exemplo.

Tucker então liga a cripto não a um bem concreto, mas a um serviço concreto que cumpre com uma necessidade profunda e possui utilidade direta – a saber, a blockchain como um sistema de pagamento.

> Bitcoin é tanto um sistema de pagamento quanto uma moeda. O sistema de pagamento é a fonte de valor [não-monetário], enquanto a unidade de medida expressa esse valor em termos de preço. A unidade de dinheiro e de pagamento é sua característica mais incomum, é aquela que a maioria dos comentadores teve dificuldade em entender [...]. Essa lacuna entre dinheiro e pagamento sempre esteve conosco, exceto no caso de proximidade física. Se eu lhe der um dólar por seu pedaço de pizza, não há terceira parte. Mas sistemas de pagamentos, terceiros, e relacionamentos de confiança se tornam necessários uma vez que você deixa a proximidade geográfica. É aí que as companhias como a Visa e instituições como bancos se tornam indispensáveis.

Para Tucker, o valor não-monetário da cripto é um sistema de pagamento que não requer uma terceira parte confiável e não possui limitações geográficas. A blockchain é o que faz a cripto emergir como um meio de troca. Dessa maneira, o Teorema da Regressão é aplicado ao bitcoin, mas o teorema precisa ser atualizado para focar nos serviços únicos – funcionando como bens de facto – que estão disponíveis na era digital.

A última palavra do Teorema da Regressão pertence a Satoshi. Em um post intitulado "Bitcoin does NOT violate Mises' Regression Theorem" no fórum bitcointalk que ele fundou, Satoshi afirma:

> Como um experimento mental, imagine que houvesse um metal base tão escasso quanto o ouro, mas com as seguintes propriedades: – de cor acinzentada – não é um bom condutor de eletricidade – não é particularmente forte, mas também não é dúctil ou facilmente maleável – não é útil para qualquer propósito prático ou ornamental e tem uma propriedade mágica especial: – pode ser transportado através de um canal de comunicação. Se, de alguma forma, adquirisse algum valor por qualquer motivo, qualquer pessoa que quisesse transferir riqueza a longa distância poderia comprá-la, transmiti-la e fazer com que o destinatário a vendesse. Talvez possa obter um valor inicial circularmente como você sugeriu, por pessoas prevendo sua potencial utilidade para

> troca. (Eu definitivamente gostaria de alguns) Talvez colecionadores, qualquer motivo aleatório poderia desencadear isso. Creio que as qualificações tradicionais para dinheiro foram escritas com a suposição de que existem tantos objetos concorrentes no mundo que são escassos, um objeto com o bootstrap automático de valor intrínseco certamente vencerá aqueles sem valor intrínseco. Mas se não houvesse nada no mundo com valor intrínseco que pudesse ser usado como dinheiro, apenas escasso, mas sem valor intrínseco, penso que as pessoas ainda aceitariam algo. (Estou usando a palavra escasso aqui apenas para significar oferta potencial limitada).

Mesmo se a cripto for uma moeda corrente válida, ela precisa poder competir com a moeda fiduciária e com outras moedas se ela quiser prosperar. O que faz uma moeda competitiva? Isso leva à questão mais fundamental de "O que é dinheiro?"

O Dinheiro pode criar Libertação e Civilização […] ou Opressão

> Historicamente, o dinheiro foi uma das primeiras coisas controladas pelo governo, e a "revolução" de livre mercado dos séculos XVIII e XIX fez muito pouco efeito na esfera monetária. Portanto, é hora de voltarmos a atenção fundamental para o sangue vital de nossa economia – o dinheiro.
> – Murray Rothbard, *What Has Government Done to Our Money?*

Eu tinha sete anos de idade quando percebi que meus pais não entendiam algumas das dinâmicas mais importantes da vida. Eu estava no banco de trás do nosso carro com um saco de doces que havia sido comprado em uma loja de beira de estrada na esperança de me manter quieta. Não funcionou. Um pensamento escapou pela minha boca: "Por que pagamos por tudo? Por que as pessoas simplesmente não vão para as lojas e pegam o que precisam?"

Minha mãe respondeu: "É errado roubar."

Expliquei: "Não quero dizer roubar. Quero dizer, por que damos dinheiro às pessoas em vez de apenas compartilhar tudo?" Meus pais ficaram em silêncio.

Quando perguntei novamente, minha mãe respondeu por cima do ombro: “Não faça perguntas idiotas!”

Eles não sabiam a resposta; eu reconheci isso imediatamente. E sua incapacidade de explicar por que precisávamos de dinheiro me perturbou porque eles discutiam sobre dinheiro constantemente. Havia o suficiente para consertar o carro e para pagar a hipoteca? Eles poderiam se dar ao luxo de substituir o telhado? Qual foi o teto de gastos no Natal deste ano? O dinheiro era um tema em todos os aspectos de suas vidas e ainda assim meus pais não sabiam como responder à pergunta básica do porquê precisamos dele.

“O dinheiro é como o mundo funciona”, meu pai finalmente explicou, “porque permite que as pessoas comprem as coisas de que precisam para viver.” Esta foi uma não-resposta porque me fez não entender por que compramos coisas em vez de simplesmente compartilhá-las. Em um nível infantil, eu estava tentando entender a teoria monetária, e tenho lutado com isso desde então.

Nada foi mais benéfico nesta busca do que o pequeno livro *What Has Government Done to Our Money?* por Rothbard. Ele não usou o termo “terceira parte confiável” ou seu equivalente no livro ou em qualquer outro lugar em seus escritos, até onde eu saiba. Murray era um amigo e mentor, no entanto, o que me dá alguma confiança em prever qual teria sido sua provável reação a toda a hipótese de Satoshi. Suspeito que ele não teria visto a necessidade de confiar em um intermediário financeiro como um problema porque os bancos privados podiam oferecer garantias como reputação, resgate em ouro e auditorias. Para Murray, o dilema do dinheiro moderno parecia começar com a moeda fiduciária do governo como o problema, e terminou com o livre mercado como a solução que permitia às instituições financeiras privadas e à moeda emitida por indivíduos, caso optassem por fazê-lo. O nome de Murray para sua própria moeda hipotética era “The Rothbard”.

What Has Government Done to Our Money? Pertence aos anos pré-Bitcoin, mas oferece contribuições significativas para a cripto. Explica as origens do dinheiro em termos claros, bem como destaca o papel proeminente do dinheiro em estabelecer a libertação e a civilização. O livro providencia um contexto no qual apreciar a imensa liberação que é a cripto e a imensa opressão que é a moeda fiduciária. O livro é uma exposição enganosamente simples da maior fraude do mundo: a

inflação. O golpe só é possível quando as pessoas precisam de uma terceira parte confiável em assuntos financeiros e o governo usurpa esse papel por meio da lei e do banco central.

Compreender a inflação requer uma compreensão de bom senso do que é dinheiro e do que deveria ser. Isso não é pouca coisa. A teoria monetária moderna cria uma névoa de complexidade que garante que as pessoas comuns fiquem sem palavras quando confrontadas com questões básicas – mesmo aquelas que impactam profundamente suas vidas. Isso poderia ser evitado facilmente. As escolas poderiam ensinar economia prática; o governo e as instituições financeiras poderiam ser transparentes em vez de paredes de tijolos; a política fiscal poderia ser apresentada em inglês em vez de em burocratês com estatísticas e matemática impenetráveis.

Isso não acontecerá por si só. A falta de conscientização pública beneficia o monopólio monetário do estado e as escolas públicas financiadas por impostos não são propensas a ensinar a revolução contra a mão que as alimenta.

Um Breve Tour Pelo Básico

Toda sociedade comercializa bens e serviços porque a troca é uma necessidade humana. É o motor da vida econômica, uma fonte de prosperidade e a base da sobrevivência. O comércio não é um jogo de soma zero, como argumentam alguns economistas. Ou seja, se uma pessoa troca um peixe por um pão, o lucro de um comerciante não anula o do outro. O comércio é uma situação ganha-ganha porque a troca só ocorre quando uma pessoa valoriza mais o pão do que o peixe e vice-versa. Ou cada um ganha com a troca ou ela não ocorre. No processo, os comerciantes também estabelecem cooperação e, talvez, um nível de boa vontade que ajude o comércio no futuro. Isso torna o livre trocar um dos principais alicerces da sociedade civil.

Os seres humanos são tão magnificamente variados que existe uma gama diversificada de habilidades mesmo dentro de um pequeno grupo de indivíduos. Negociar essas habilidades aumenta as chances de sobrevivência tanto para o grupo quanto para cada membro dele, mas a troca direta ou troca é severamente falha, como explica Rothbard. “Os dois problemas básicos são ‘indivisibilidade’ e ‘falta de coincidência de quereres’.” “Indivisibilidade” significa que um bem de troca, como um arado, pode ser difícil ou impossível de dividir em muitas partes, o que

impede que seja trocado por várias coisas com várias pessoas. Então, nenhuma negociação ocorre. "Uma falta de coincidência de quereres" significa que Smith possui ovos e Jones possui sapatos, mas Smith quer manteiga. Assim, nenhuma negociação ocorre.

A troca indireta resolve o problema do escambo [...] até certo ponto. Smith troca seus ovos pelos sapatos de Jones porque o último pode ser trocado por uma terceira pessoa por algo que Smith *deseja*. Isso mitiga a falta de coincidência de quereres. Mais importante, para a teoria monetária, entretanto, negociações indiretas naturalmente encorajam um meio de troca a emergir. Por quê? Negociadores irão favorecer itens de escambo que são altamente desejáveis e serão aceitos por muitas pessoas. Bens altamente trocáveis tendem a partilhar de características, incluindo divisibilidade, durabilidade, fungibilidade e transportabilidade. Não coincidentemente, essas mesmas características frequentemente descrevem bom dinheiro, e elas se aplicam a cripto.

De acordo com o teorema de Mises, um item de escambo desejável é primeiro valorado por seu valor de uso. Rothbard lista algumas mercadorias que se tornam moedas. "[O] tabaco na Virgínia colonial, açúcar nas Índias Ocidentais, Sal na Abissínia, gado na Grécia Antiga, pregos na Escócia, cobre no antigo Egito, e grãos, contas, chá, moluscos e anzóis." A demanda por um bem gera uma "espiral de reforços: mais mercabilidade causa um uso mais amplo como um meio o qual causa mais mercabilidade etc. Eventualmente, uma ou duas mercadorias são usadas como meio geral – em quase todas as trocas – e essas são chamadas de dinheiro".

Moedas comumente aceitas eliminam a necessidade tanto por escambo quanto por troca indireta, as quais podem ser confusas, consumidoras de tempo e geograficamente limitadas. Moedas criam um livre mercado complexo que permite que bilhões de pessoas que não conhecem umas às outras consumam produtos ao redor do mundo. Em resumo, o dinheiro lança os seres humanos da sobrevivência para a prosperidade e possibilita o luxo do tempo para pensar, para criar arte, gozar de profundos relacionamentos e tomar conta de sua saúde. Um meio de troca é um dos fundamentos da civilização.

E então entra o governo. A moeda desempenhou um papel definidor em libertar e civilizar os seres humanos. Agora seria usada para escravizá-los.

Inflação, o Maior Roubo de Todos

O governo não produz bens e serviços no mercado para vender aos clientes que os desejam. Indivíduos fazem isso. O estado rouba riqueza dos chamados clientes, forçando-os a pagar por “bens” e “serviços”, como os militares, quer queiram ou não. A tributação é a forma mais visível de roubo. Mas está longe de ser o único motor de roubo. Ao paralisar os concorrentes que supririam as necessidades da sociedade no livre mercado, o governo também rouba oportunidades e lucros não realizados da classe produtiva das pessoas.

A ferramenta mais poderosa de roubo público, no entanto, é o monopólio do estado na emissão de dinheiro ou fiduciário. Rothbard explica: “O surgimento do dinheiro, enquanto um benefício para a raça humana, também abriu uma rota mais sutil para a expropriação governamental de recursos […] [Se] o governo puder encontrar maneiras de se envolver em falsificação – a criação de dinheiro novo do nada – ele pode rapidamente produzir seu próprio dinheiro sem se dar ao trabalho de vender serviços ou minerar ouro. Ele pode então se apropriar de recursos astutamente e passar quase desapercebido, sem despertar a hostilidade desencadeada pela tributação.”

A parte “quase desapercebida” da análise anterior é fundamental. Todo mundo entende de tributação porque vem com formulários para preencher, deduções de um salário, prisão por sonegação, agentes assustadores que auditam e um acréscimo doloroso sobre mercadorias na caixa registradora. Quase todo mundo se ressente da tributação; surtos de resistência, rebeliões e pedidos de revogação são temas comuns ao longo da história; a Revolução Americana é um exemplo. Previsivelmente, o governo quer reduzir a presença de multidões enfurecidas que protestam contra suas políticas nas ruas. No entanto, ele precisa dessa riqueza.

Em contraste, uma espiral complexa e arcana de inflação raramente enfurece a pessoa comum que não a percebe até que os efeitos sejam aparentes, ruinosos e inescapáveis. Se a tributação é o equivalente ao roubo com uma arma apontada para a cabeça das pessoas, então a inflação é um ladrão que despoja suas casas na madrugada. A inflação também é difícil de evitar porque os monopólios governamentais incorporaram o decreto e o sistema bancário central no centro do comércio moderno. Talvez o conhecido ditado deva ser “nada é inevitável, exceto a morte e a inflação”.

O que é inflação? A inflação é um aumento na oferta de dinheiro e de crédito. Geralmente ela está associada ao governo, e com razão, mas também pode ocorrer com o dinheiro do livre mercado. A oferta de ouro pode aumentar por vários motivos, incluindo enormes descobertas minerais ou uma liberação maciça de reservas de um banco. Mas uma diferença crucial entre a inflação do estado e o livre mercado é que o ouro cumpre com muitos usos não monetários. Se a oferta aumentar, o consumo para esses usos também aumentará, pois o custo do ouro cairá. Isso significa que uma inflação nas unidades de ouro disponíveis seria uma coisa boa para algumas pessoas – especificamente para aqueles que usam ouro de maneira não monetária. Por sua vez, o aumento da demanda por ouro não monetário absorveria o "excesso" de oferta e elevaria o valor monetário. A inflação de livre mercado é autoajustável e é acompanhada por um benefício social, incluindo um aumento no valor de moedas privadas concorrentes, como a prata.

Por outro lado, o único uso da moeda fiduciária é como dinheiro. Isso significa que não há mecanismo de autoajuste. Os mercados mundiais podem desvalorizar uma moeda fiduciária notória se outras moedas fiduciárias não forem ainda piores. Nessa circunstância, no entanto, o governo com moeda desvalorizada pode aumentar sua impressora e criar um círculo vicioso de inflar ainda mais a oferta monetária. A inflação fiduciária não é autoajustável nem oferece benefícios a ninguém, exceto a classe de elite que recebe primeiro o dinheiro recém-impresso.

Para a pessoa média, a palavra "inflação" é sinônimo de "aumento de preços", mas o aumento é uma consequência da inflação, não um sinônimo dela. Como observado anteriormente, a inflação é simplesmente um aumento na oferta de dinheiro e de crédito. A diferença entre esses dois significados é muito mais do que semântica. Ver a inflação como um aumento de preços ignora muito do grande dano infligido pela inflação porque implica que toda a sociedade enfrenta a mesma desvantagem: preços mais altos onipresentes. O oposto é verdadeiro. A inflação é uma arma de classe que redistribui a riqueza das pessoas médias para a elite da sociedade. Isso acontece porque o novo fiat é inicialmente avaliado na mesma proporção que as unidades antigas que já estão em circulação. Dobrar a oferta de dinheiro da noite para o dia acabaria colapsando o poder de compra de cada unidade em circulação, mas o prazo operacional é "eventualmente". Os primeiros usuários aproveitam o valor da pré-inflação porque o dano escorre lentamente

por toda a economia. Esses primeiros usuários incluem o estado, a burocracia, as instituições financeiras e as empresas compadres que recebem empréstimos favoráveis. O usuário final é a pessoa comum que recebe a moeda fiduciária diluída que perdeu poder de compra à medida que se espalhava pela economia. A pessoa comum suporta o peso da inflação por ter o valor de sua riqueza e renda caindo enquanto o custo de vida dispara. Enquanto isso, a classe alta goza de maior prosperidade às custas de todos.

Com leis de curso legal e sem o padrão ouro, pouco previne o governo de expandir o dinheiro e o crédito à vontade, usando taxas de juros para afinação. Os incentivos estão todos no lado da inflação. É altamente lucrativo ao estado e na maior parte invisível para o público, especialmente nos primeiros estágios. O vilão econômico dos defensores do livre mercado, John Maynard Keynes, soube bem disso. Seu livro pivô *The Economic Consequences of Peace* declara:

> É dito que Lenin declarou que a melhor maneira de destruir o Sistema Capitalista era perverter a moeda. Através de um contínuo processo de inflação, o governo pode confiscar, secretamente e de forma não observada, uma importante parte da riqueza de seus cidadãos. A partir desse método eles não apenas confiscam, mas o fazem arbitrariamente; e enquanto o processo empobrece muitos, ela na verdade enriquece alguns. Enquanto a inflação procede e o valor real da moeda flutua selvagemente de mês para mês, todas as relações permanentes entre devedores e credores, os quais formam o fundamento último do capitalismo, tornam-se tão totalmente desordenados que são quase sem sentido; e o processo de obtenção de riqueza degenera em jogo e loteria.
>
> Lênin certamente estava certo. Não há meio mais sutil e seguro de derrubar a base existente da sociedade do que corromper a moeda. O processo envolve todas as forças ocultas da lei econômica do lado da destruição, e o faz de uma maneira que nem um homem dentre milhões de homens é capaz de diagnosticar.

Os danos da inflação continuam. Rothbard enfatiza um menos discutido:

> Isso distorce a pedra angular da nossa economia: o cálculo empresarial. Como nem todos os preços mudam uniformemente e na mesma velocidade, torna-se muito difícil para as empresas separar o duradouro do transitório e avaliar verdadeiramente as demandas dos consumidores ou o custo das suas operações. Por exemplo, a prática contábil insere o "custo" de um ativo no valor que a empresa pagou por ele. Mas se a inflação intervir, o custo de reposição do ativo quando se desgastar será muito maior do que o registrado nos livros. Como resultado, a contabilidade das empresas irá superestimar seriamente seus lucros durante a inflação – e pode até estar consumindo capital enquanto pensa estar aumentando seus investimentos.

Os bancos centrais têm grande culpa pelo roubo e distorções da inflação; o estado é, em última análise, o culpado. Um banco central é uma câmara de compensação de moeda nacional; é um intermediário para as políticas financeiras de uma nação. Ele goza de controle monopolista sobre a produção e distribuição de dinheiro e crédito de uma nação. Normalmente, também esculpe a política monetária por meio de mecanismos, como a fixação de taxas de juros, e policia os bancos membros.

O Federal Reserve System americano às vezes é chamado de "privado". Por um lado, os Bancos de Reserva regionais são corporações privadas de propriedade dos seus bancos membros. O rótulo é ilusório. O Federal Reserve foi estabelecido por um ato do Congresso em 1913 e deriva o seu poder principal de um monopólio garantido pelo governo para emitir curso legal. O sistema pode imitar uma agência privada em alguns modos, mas, como explica Rothbard, o sistema de bancos é "sempre dirigido por oficiais apontados pelo governo, e servem como braços do governo."

O Federal Reserve permite a inflação. Ele o faz de duas maneiras básicas: removendo as restrições à inflação e direcionando a própria inflação. Rothbard esboçou uma implantação inicial da primeira tática. "[O] Federal Reserve Act compele os bancos a manter a proporção mínima de reservas para depósitos e, desde 1917, essas reservas só podiam consistir em depósitos no Federal Reserve Bank. O ouro não podia mais

fazer parte das reservas legais de um banco; tudo teve que ser depositado no Federal Reserve Bank". Rothbard ilustra a segunda tática de direcionar a inflação. "Ao controlar as 'reservas' dos bancos – suas contas de depósito no Banco Central. Os bancos tendem a manter uma certa proporção de reservas para seus passivos totais de depósito, e nos Estados Unidos o controle do governo é facilitado pela imposição de uma proporção mínima legal ao banco. O Banco Central pode estimular a inflação, então, despejando reservas no sistema bancário, e reduzindo o índice de reservas, permitindo assim uma expansão do crédito bancário nacional."

Na medida em que o governo aperta as rédeas sobre o dinheiro, a liberdade e a civilização são enfraquecidas. O dinheiro privado tradicional confronta e supera a fiat do governo. Mas enquanto o estado puder dominar e manipular o dinheiro, ele pode possuir o sistema financeiro ao ponto de chegar em contas bancárias individuais, títulos e outras riquezas armazenadas de indivíduos. Ele pode possuir sua riqueza futura diluindo-a através da inflação. Até as criptos, o anarquismo tropeçou e caiu sobre o problema de terceiras partes confiáveis do estado e dos bancos. Até as criptos, o estado parecia ter um controle inabalável da moeda.

Liberdades Civis e Bancos Centrais

O sistema bancário central deve ser rejeitado não apenas por motivos econômicos, mas também por motivos de liberdade civil. (Nota: Eu não faço distinção entre direitos econômicos e civis. Ambos são expressões da propriedade de si; essa é a jurisdição moral que todo ser humano tem sobre seu próprio corpo e ações pacíficas simplesmente em virtude de ser humano. Mas fazer uma distinção entre direitos econômicos e civis é comum)

O sistema bancário central é um veículo de controle monetário e financiamento para todos no poder. De acordo com o *Financial Times* –, "Os principais bancos agora possuem um quinto da dívida total do governo". Os seis principais bancos centrais "que embarcaram na flexibilização quantitativa na última década – o Federal Reserve dos EUA, o Banco Central Europeu, o Banco do Japão e o Banco da Inglaterra, juntamente com os bancos centrais suíços e suecos – agora detêm mais de US $15 trilhões em ativos, de acordo com a análise do FT do FMI e dos números do banco central, mais de quatro vezes o nível pré-crise".

A flexibilização quantitativa ocorre quando um banco central compra títulos, geralmente do governo, para reduzir as taxas de juros e aumentar a oferta de moeda. Isso alimenta artificialmente a economia, reduzindo os custos de empréstimos para famílias e empresas. Mas isso é insustentável.

Governos e bancos centrais não são independentes. A história revela que o conluio entre eles é inerente e íntimo, não acidental. O sueco Riksbank é amplamente considerado como o primeiro banco central. Inaugurado em 1668, o Riksbank era tecnicamente um banco privado de ações conjuntas, mas funcionava sob estrita autoridade real; o rei determinou as regras de operação e nomeou a administração do banco. Todo o propósito do Riksbank era emprestar fundos ao governo e ser uma câmara de compensação para o comércio.

Em 1694, a Governança e a Companhia do Banco da Inglaterra foram criadas pelo Royal Charter. É um modelo sobre o qual a maioria dos bancos centrais se baseiam. O Banco da Inglaterra surgiu porque o crédito do rei William III estava mal. A sociedade por ações forneceu um caminho para o rei arrecadar os fundos públicos que lhe permitiram continuar travando a guerra. William III estava em desacordo militar com a Irlanda, Escócia e América do Norte, todos em vários estágios de rebelião. Mais importante ainda, no entanto, a Guerra dos Nove Anos (1688-1697) com a França devastou a marinha da Inglaterra. Nenhuma instituição financeira arriscaria as 1,2 milhões de libras necessárias para reconstruí-la.

Assim, a lei inglesa estabeleceu incentivos artificiais para encorajar empréstimos ao rei. Aqueles que auxiliam no processo foram incorporados como coproprietários do Banco da Inglaterra. Os credores davam dinheiro vivo congelado ao rei em troca do qual recebiam acesso exclusivo às finanças do governo. O banco também se tornou a única empresa de responsabilidade limitada autorizada a emitir notas, usando títulos do governo como garantia. Em outras palavras, o Banco da Inglaterra concedeu um empréstimo a um beneficiário que ninguém mais tocaria; adquiriu títulos do rei – o destinatário intocável; com base nos títulos, o banco emitiu dinheiro que foi emprestado novamente. Sem privilégio legal, o banco central não teria atraído investidores ou finanças. Com o privilégio legal, os £1,2 milhão foram arrecadados em menos de duas semanas.

Governo e bancos centrais lavam as mãos uns dos outros.

O ganho financeiro não é o único motivo para atrair pessoas para a terceira parte confiável dos bancos centrais. Há também a sede por poder. A guerra é o último desdobramento de poder através do qual os governos mantêm, asseveram e expandem a si mesmos. A guerra requer dinheiro – muito. A questão é sempre como conseguir o suficiente. Existe a opção do roubo descontrolado, é claro. A economia pode ser saqueada, mas os indivíduos saqueados podem objetar e se rebelar. Tal rebelião levou à Carta Magna em 1215; um comentador da época advertiu ao rei João, “Com as ocasiões de suas guerras, ele os pilha [o povo e os nobres] com impostos e impostos até os ossos”. João foi forçado a assinar a Carta Magna, presumivelmente sob ameaça de morte. Ele prometeu parar de pilhar a economia para pagar por suas guerras. Era necessária mais sutileza na pilhagem.

Quando um governo declara guerra, ele o faz em pelo menos três frentes: o governo oponente, o povo da nação oponente e os dissidentes dentro de sua própria população. Alguns dissidentes internos agitam, a princípio, mas suas fileiras são engrossadas por aqueles que se opõem aos impostos e outras violações da liberdade civil cometidas em nome da guerra. Para o governo, a questão complicada é: como extrair o máximo de dinheiro possível sem incorrer em uma reação negativa? Como isso pode contornar a tendência das pessoas de afirmar suas liberdades civis e resistir?

Um aspecto pouco discutido dos bancos centrais e da manipulação da moeda é seu impacto nas liberdades civis. Impostos diretos, confiscos e regulações são visíveis. As pessoas entendem uma mão que vai direto para seus bolsos ou as joga na cadeia por se recusarem a pagar impostos pela guerra. Por outro lado, políticas monetárias confusas e não transparentes são invisíveis. As pessoas não entendem nem sentem imediatamente o impacto da flexibilização quantitativa, por exemplo. Elas não os levam para as ruas com placas de piquete. Em vez disso, as pessoas seguem suas vidas diárias e simplesmente assumem o ônus de um imposto indireto que não entendem muito bem.

Para reafirmar este ponto através de um paralelo: A inflação é um imposto oculto que as pessoas tendem a tolerar mesmo que se rebelem contra um imposto direto. A inflação é, no entanto, comparativamente invisível e não compreendida. As pessoas que protestariam contra um imposto pró-guerra toleram as políticas do banco central, sem as quais a guerra seria impossível. Aqueles que são antiguerra devem pedir, em primeiro lugar, a dissolução do Federal Reserve e de todos os outros

bancos centrais. Mas o papel dos bancos centrais no financiamento da guerra é invisível, o que permite ao governo evitar um confronto com ativistas antiguerra. As pessoas não reivindicam seus direitos civis por nenhuma outra razão além de não saberem que esses direitos estão sendo violados. O papel dos bancos centrais no controle social permanece em grande parte desconhecido porque é misterioso.

A Tecnologia Encontra a Anarquia, e Ambos Lucram

> "O Bitcoin é o catalisador para uma anarquia pacífica e libertadora. Foi feito como uma reação contra governos corruptos e instituições financeiras. Não foi somente criado em prol de melhorar a tecnologia financeira. Mas algumas pessoas adulteram a verdade. Em realidade, o Bitcoin era para funcionar como uma arma monetária, como uma criptomoeda posta para minar autoridades. Agora, ele está eufemizado. É visto como uma tecnologia educada e despretensiosa para apaziguar políticos, banqueiros e mães corujas. Seu propósito às vezes é ocultado para tornar a tecnologia palatável para as massas ignorantes e a elite do poder. No entanto, ninguém deve esquecer ou negar porque o protocolo foi escrito."
> – Sterlin Lujan

A cripto foi criada para fazer uma diferença política e não para obter lucro. Se os principais desenvolvedores quisessem colher uma fortuna, não teriam empregado software de código aberto e evitado as patentes que os tornariam bilionários. Lucrar com cripto e blockchain são subprodutos louváveis para alguns, e aqueles que acumularam riquezas no livre mercado devem ser aplaudidos. Isso é especialmente verdade porque a maneira como eles ganharam dinheiro não interferiu na privacidade e na liberdade financeira de ninguém. Da mesma forma, a blockchain não foi forjada para tornar o sistema bancário mais eficiente, mas para torná-lo obsoleto. Qualquer um que acredite que o Bitcoin foi designado para ganho financeiro não está prestando atenção à sua história ou ao idealismo embutido em seus algoritmos. O Bitcoin foi concebido como um veículo para criar mudanças políticas e sociais, empoderando indivíduos e empobrecendo o governo. Seus desenvolvedores eram revolucionários. O Bitcoin foi seu golpe de abertura.

E não foi sequer um momento antes da hora. A Internet deu ao governo uma arma incrível contra a privacidade dos indivíduos, que teria sido radicalmente reduzida sem a criptografia – a arte da comunicação secreta.

A História do Bitcoin

A história do Bitcoin às vezes é rastreada até o engenheiro e cientista Timothy C. May. O "Manifesto Cripto-Anarquista" (1988) de May apareceu pela primeira vez sendo distribuído por alguns tecno-anarquistas na conferência Crypto '88. O manifesto de seis parágrafos exige uma tecnologia de computador baseada em protocolos criptográficos que "alterariam completamente a natureza da regulamentação governamental, a capacidade de tributar e controlar as interações econômicas, a capacidade de manter a informação em segredo e até alterar a natureza da confiança e reputação … A tecnologia para essa revolução – e certamente será uma revolução social e econômica – existiu em teoria na última década.… Mas só recentemente as redes de computadores e os computadores pessoais atingiram velocidade suficiente para tornar as ideias praticamente realizáveis."

O manifesto conclui com um grito de guerra. "Levante-se, você não tem nada a perder a não ser suas cercas de arame farpado!"

Mesmo em 1988, May podia contar com uma rica história das criptos. Em meados da década de 1970, a criptografia deixou de ser domínio quase exclusivo das agências militares e de inteligência, que operavam em grande parte em sigilo. Em contraste, a pesquisa acadêmica que mais tarde surgiu foi abertamente compartilhada. Um evento em particular quebrou o controle do governo em campo. Em 1975, o guru da computação Whitfield Diffie e o professor de engenharia elétrica Martin Hellman inventaram a encriptação de chave pública e publicaram seus resultados no ano seguinte no ensaio "New Directions in Cryptography". (O que pode ser disputado porque a chave pública foi uma reinvenção, pois os britânicos haviam desenvolvido essa encriptação anteriormente, mas foram silenciados sobre o assunto pelo governo). Em 1977, os criptógrafos Ron Rivest, Adi Shamir e Leonard Adleman criaram o algoritmo de encriptação RSA, aquele que foi um dos primeiros sistemas práticos de chave pública.

A encriptação de chave pública atingiu a comunidade de computadores como uma explosão. Seu brilho é sua simplicidade. Cada usuário tem duas chaves – uma pública e uma privada – ambas únicas. A chave pública embaralha o texto de uma mensagem que pode ser decifrada apenas pela chave privada. A chave pública pode ser jogada ao vento, mas a chave privada deve ser bem guardada. Na época, o resultado estava próximo de uma privacidade impenetrável.

Diffie se inspirou no problema das terceiras partes confiáveis. O livro *High Noon on the Electronic Frontier*: *Conceptual Issues in Cyberspace* (1996) o cita dizendo: “Você pode ter arquivos protegidos, mas se uma intimação fosse enviada ao gerente do sistema, daí não viria nada de bom. Os administradores o dedurariam, porque não teriam interesse em ir para a cadeia.” Sua solução foi eliminar a necessidade de confiança por meio de uma rede descentralizada na qual cada indivíduo possui a chave matemática de sua própria privacidade – o direito mais ameaçado pela sociedade digital. A encriptação de chave pública também removeu a tensão de enviar informações seguras por canais inseguros. Excluiu “Eve”; esse é o nome que os criptógrafos chamam de bisbilhoteiro indesejado que pode ser o estado ou um criminoso comum. É importante ressaltar que a criptografia de chave pública era gratuita para todos porque uma revolução bem-sucedida não requer nada além de participação.

O governo não achou graça. A Agência de Segurança Nacional (NSA) não podia mais espionar à vontade porque seu monopólio doméstico de criptografia foi subitamente arrancado. O jornalista Steven Levy comentou em um artigo da *Wired*: “Em 1979, Inman [então chefe da NSA] deu um discurso que veio a ser conhecido como ‘the sky is falling’, alertando que ‘atividades criptológicas e publicações não governamentais [...] representam riscos claros para a segurança nacional’.”

Uma declaração posterior do criptógrafo John Gilmore capturou a resposta dos rebeldes:

> Mostre-nos. Mostre ao público como sua capacidade de violar a privacidade de qualquer cidadão evitou um grande desastre. Eles estão restringindo a liberdade e a privacidade de todos os cidadãos para nos defender contra um bicho-papão que eles não explicaram. A decisão de literalmente trocar nossa privacidade é uma decisão que deve ser tomada por toda a sociedade, não unilateralmente por uma agência de espionagem militar.

O que poderia ser chamado de “a primeira guerra cripto” estourou quando a NSA tentou restringir a circulação das ideias de Diffie e Hellman. A agência informou aos editores que os dois rebeldes e qualquer um que os publicasse poderia enfrentar pena de prisão por violar as leis

que restringem a exportação de armas militares. Um dos veículos de Hellman, o Instituto de Engenheiros Elétricos e Eletrônicos (IEEE), recebeu uma carta que dizia, em parte: “Percebi nos últimos meses que vários grupos do IEEE têm publicado e exportado artigos técnicos sobre *encriptação e criptologia* – um campo técnico que é coberto por Regulamentos Federais, a saber: ITAR (Regulamento Internacional de Tráfego de Armas, 22 CFR 121-128).” Ordens de mordaça foram emitidas. Legalização foi proposta. A NSA tentou controlar o financiamento para pesquisa de cripto e considerou exigir que as pessoas depositassem suas chaves privadas em um terceiro que seria vulnerável à ordem de um juiz ou à polícia. Isso teria retornado ao problema de terceiras partes confiáveis que a criptografia de chave pública pretendia evitar. Em reação, o cofundador da Electronic Frontier Foundation, John Perry Barlow, declarou: “Você pode ter meu algoritmo de encriptação […] quando você arrancar meus dedos frios e mortos da minha chave privada.”

A NSA falhou. A encriptação potente tornou-se um bem público que oferecia privacidade extraordinária aos indivíduos.

Levantem-se, Cypherpunks!

No final da década de 1980, os cypherpunks surgiram como algo semelhante a um movimento. O rótulo deliberadamente bem-humorado foi cunhado pela hacker Judith Milhon, que misturou “cipher” com “cyberpunk”. Os cypherpunks queriam a criptografia para se defender tanto da vigilância quanto da censura do estado. Eles também buscaram construir uma sociedade contra econômica como uma alternativa aos sistemas bancários e financeiros existentes. Conforme definido por seu exemplar e Anarcocapitalista Samuel E. Konkin III, a contra economia é o estudo e a prática de toda ação humana pacífica que é proibida pelo estado.

A visão dos cypherpunks foi facilitada pelo trabalho pioneiro do cientista da computação David Chaum, apelidado de “Houdini da cripto”. Três de seus artigos foram particularmente influentes.

- Correio Eletrônico não Rastreável, Endereços de Retorno e Pseudônimos Digitais” (1981) estabelece as bases para a pesquisa e o desenvolvimento de comunicações anônimas baseadas em criptografia de chave pública.

- "Assinaturas Cegas para Pagamentos não Rastreáveis" (1983) afirma: "A automação da forma como pagamos por bens e serviços já está em andamento. […] A estrutura final do novo sistema de pagamentos eletrônicos pode ter um impacto substancial na privacidade pessoal, bem como na natureza e extensão do uso criminoso de pagamentos. Idealmente, um novo sistema de pagamentos deve abordar esses dois conjuntos de preocupações aparentemente conflitantes." O ensaio clama por dinheiro digital.
- "Segurança sem Sistemas de Transação para tornar o Grande Irmão Obsoleto" (1985) descreve ainda mais dinheiro digital anônimo e sistemas de reputação com pseudônimos.

Um típico cypherpunk desconfiava e não gostava do governo, especialmente do tipo federal; a cruzada da NSA contra a encriptação privada só fortaleceu essa resposta. A maioria dos cypherpunks também abraçou a contracultura com sua ênfase na liberdade de expressão, liberação sexual e liberdade de usar drogas. Em suma, eles eram libertários civis. Um dos primeiros retratos dos radicais de codificação foi o artigo de Levy *Wired* mencionado anteriormente. Levy os chamou de "libertários techie-cum-civil". Eles eram idealistas que "esperam por um mundo onde as pegadas informativas de um indivíduo – desde uma opinião sobre aborto até o registro médico de um aborto real – possam ser rastreadas apenas se o indivíduo envolvido optar por revelá-las; um mundo onde mensagens coerentes são lançadas ao redor do globo por redes e micro-ondas, mas intrusos e federais que tentam arrancá-las da fumaça encontram apenas rabiscos; um mundo onde as ferramentas de espionagem são transformadas em instrumentos de privacidade." As apostas? "O resultado dessa luta pode determinar a quantidade de liberdade que nossa sociedade nos concederá no século XXI." O ideal não é que a liberdade lhes seja dada, é claro, mas que ela seja tomada como um direito natural.

Em 1991, Phil Zimmermann desenvolveu o Pretty Good Privacy (PGP), que se tornou o software mais popular do mundo de encriptação de e-mail. Ele via o PGP como uma ferramenta de direitos humanos e acreditava tanto nele que perdeu cinco pagamentos de hipoteca e quase perdeu sua casa para projetá-la. A versão original foi chamada de "uma teia de confiança". Zimmermann descreve este protocolo no manual do PGP versão 2.0.

> Com o passar do tempo, você acumulará chaves de outras pessoas que você pode querer designar como apresentadores confiáveis. Todos os outros escolherão seus próprios apresentadores confiáveis. E todos irão acumular e distribuir gradualmente com suas chaves uma coleção de assinaturas de certificação de outras pessoas, com a expectativa de que qualquer pessoa que a receba confie em pelo menos uma ou duas das assinaturas. Isso causará o surgimento de uma rede de confiança descentralizada e tolerante a falhas para todas as chaves públicas.

O PGP foi inicialmente distribuído gratuitamente por ser postado em quadros de avisos de computador. Zimmermann explicou: "[c]omo milhares de sementes de dente-de-leão soprando no vento" o PGP se espalhou pelo mundo. O governo percebeu, e Zimmermann foi alvo de uma investigação criminal de três anos com base na possível violação das restrições dos EUA de exportação de software criptográfico.

Saltando para 1992. May, Milhon, Gilmore e Eric Hughes formaram um pequeno grupo de fanáticos por programação que se reuniam todos os sábados em um pequeno escritório em São Francisco. Um artigo do *Christian Science Monitor* descreve o grupo como "todos unidos por aquela combinação única da Bay Area: apaixonados por tecnologia, mergulhados na contracultura e inabalavelmente libertários."

O grupo cresceu rapidamente. Um fórum de postagem eletrônico chamado The List tornou-se seu aspecto mais ativo, com os "algoritmos das pessoas" atraindo forte apoio de nomes como Julian Assange e Zimmermann. O *Christian Science Monitor* comenta: "Os libertários radicais dominaram a lista, junto com 'alguns anarcocapitalistas e até alguns socialistas'. Muitos tinham capacidade técnica de trabalhar com computadores; alguns eram cientistas políticos, estudiosos dos clássicos ou advogados". Eric Hughes contribuiu com outro manifesto para o movimento. "A Cypherpunk's Manifesto" começa, "A privacidade é necessária para uma sociedade aberta na era eletrônica". Ele continua, "pois para a privacidade ser amplamente espalhada ela precisa ser parte de um contrato social. As pessoas precisam se juntar e implantar esses sistemas pelo bem comum. A privacidade só se estende até a cooperação de seus companheiros na sociedade."

O grupo rapidamente encontrou uma objeção que viria a dominar o ataque do governo à encriptação privada; "maus agentes", argumentou-se, usarão o anonimato para cometer crimes. Durante uma entrevista em 1992, um cético confrontou May. "Parece a coisa perfeita para notas de resgate, ameaças de extorsão, subornos, chantagem, informações privilegiadas e terrorismo", ele desafiou e May respondeu: "Bem, e quanto à venda de informações que não são vistas como legais, digamos, sobre cultivo de maconha e aborto do tipo faça você mesmo"? E quanto ao anonimato desejado para denunciantes, confessionários e namoros?" E enquanto aos "bons agentes" que seriam penalizados pela remoção da criptografia privada?

Cypherpunks acreditavam que a criptografia de chave pública realmente tornava a sociedade *menos* perigosa e menos criminosa porque reduziu ou eliminou pelo menos duas grandes fontes de violência. A primeira foi o estado; sua intrusão criminosa na vida pessoal dos indivíduos poderia ser amplamente neutralizada pela privacidade efetiva. Se as trocas financeiras fossem invisíveis, por exemplo, o roubo de impostos ou o confisco seria impossível. A segunda fonte de violência era o risco associado a crimes sem vítimas, como o uso de drogas, que não eram vistos pelos cypherpunks como crimes. A encriptação de chave pública reduziu ou removeu esse risco. Encomendar drogas on-line, por exemplo, era mais seguro do que comprá-las em um beco de um bairro ruim à meia-noite.

Sem dúvida, a criptografia de chave pública poderia proteger atividades que *violavam* direitos, assim como pagar em dinheiro vivo poderia fazê-lo. No entanto, essa perspectiva era amplamente irrelevante, já que a encriptação era uma realidade que se espalharia apesar dos efeitos colaterais desagradáveis. Os Cypherpunks argumentaram que a tecnologia ou a comunidade poderiam desenvolver soluções para crimes online reais.

As Guerras Cripto Continuam

Um incidente capturou o núcleo das guerras cripto entre os cypherpunks e o estado. Gilmore decidiu salvar e divulgar as informações em documentos ameaçados pela censura da NSA. Ele distribuiu um artigo de um criptógrafo cujo trabalho a NSA havia sido fundamental para suprimir. Depois que Gilmore postou na Internet, o artigo se tornou viral. Em 1992, Gilmore apresentou um pedido de Freedom of

Information Act (FOIA) para adquirir as partes públicas de uma obra de quatro volumes de William Friedman, que às vezes é chamado de pai da criptografia americana. Os manuais já existiam há muitas décadas. Gilmore também solicitou que os outros livros de Friedman fossem tornados públicos.

Enquanto a NSA prolongava sua resposta à FOIA, Gilmore ouviu notícias fascinantes de um amigo cypherpunk. Os documentos pessoais de Friedman foram doados para uma biblioteca depois de sua morte, e eles incluem os manuscritos anotados de um livro sigiloso. O amigo simplesmente tirou o livro da estante da biblioteca e o xerocou para Gilmore. Outro dos livros sigilosos de Friedman foi encontrado em um microfilme na Boston University. Gilmore notificou o juiz no que se tornou um apelo à FOIA, para que os assim chamados documentos classificados estivessem publicamente disponíveis em bibliotecas. Antes de fazê-lo, porém, Gilmore fez várias cópias do material em questão e as escondeu em lugares obscuros, incluindo um prédio abandonado.

A NSA reagiu com extrema veemência. Eles invadiram bibliotecas e reclassificaram documentos que estavam disponíveis publicamente. O Departamento de Justiça chamou o advogado de Gilmore para dizer que seu cliente estava perto de violar o Ato de Espionagem, o qual poderia levar a uma prisão de até 10 anos. A violação: ele mostrou às pessoas um livro de uma biblioteca pública.

Por sua vez, Gilmore contatou repórteres de tecnologia no jornal. A NSA temia a publicidade, e os cypherpunks sabiam disso. Artigos críticos da NSA começaram a fluir, incluindo um na *San Francisco Examiner*. Dois dias depois, o New York Times afirmou: "A National Security Agency, a agência de espionagem eletrônica secreta do país, recuou abruptamente de um confronto com um pesquisador independente sobre manuais técnicos secretos que ele encontrou em uma biblioteca pública há várias semanas. […] [E]la disse que os manuais não eram mais secretos e que o pesquisador poderia guardá-los". A *Aegean Park Press*, uma editora da Califórnia, rapidamente imprimiu os livros.

Os primeiros cypherpunks eram protótipos que definiram a atitude, a tecnologia e o contexto político em que grande parte da próxima geração de zelotes da cripto operou. Os objetivos eram a desobediência à autoridade injusta, contra economia, liberdade pessoal e a ruptura de um sistema corrupto por meio da criptografia.

Lições de Moral de Moedas Digitais Anteriores

> Existiram 3 fases da moeda: a baseada em mercadorias, a baseada em política e agora a baseada em matemática.
> – Chris Dixon

Versões de dinheiro digital e sistemas de transferência online existiam décadas antes do Bitcoin. A DigiCash e o e-gold estão entre os mais conhecidos, mas nenhum deles conseguiu abalar o obstinado problema de terceiras partes confiáveis. Ambos careciam do veículo essencial da privacidade e do self-banking criado por Satoshi: a blockchain. Os sistemas iniciais são úteis, entretanto, como lições de moral e realçam a elegância do Bitcoin.

DigiCash: Suas lições

Em 1983, o renomado criptógrafo David Chaum introduziu a ideia de dinheiro digital em um trabalho de pesquisa inovador. Em 1989, ele fundou uma corporação de dinheiro eletrônico chamada DigiCash, que, por sua vez, estabeleceu o sistema de pagamento eletrônico e-cash. (A moeda real foi apelidada de DigiCash). O e-cash foi chamado de "tecnicamente perfeito". Ele foi construído sobre um sistema anterior projetado por Chaum: Assinatura Cega. Essa é uma assinatura digital em que o conteúdo de uma mensagem de uma pessoa é disfarçado para que não seja visto por uma segunda pessoa que autentica a mensagem.

O processo é frequentemente descrito por uma analogia. Um eleitor quer que seu voto permaneça secreto. Para ser contado, no entanto, deve ser assinado por um funcionário eleitoral que verifica a elegibilidade do eleitor. A solução: o eleitor escreve suas credenciais do lado de fora de um envelope, embrulha a cédula marcada em papel carbono e a coloca dentro do envelope. O funcionário verifica as credenciais e assina o envelope, transferindo sua assinatura para a cédula interna; ele verifica a cédula sem saber seu conteúdo. O eleitor coloca a cédula agora autorizada em um novo envelope não marcado que é colocado em uma caixa de cédulas esperando para serem contadas. O tabulador verifica a assinatura de autenticação e o voto é registrado. O contator de votos não tem, entretanto, a menor ideia de quem colocou qualquer voto

particular. Nem o conteúdo do voto nem o próprio voto podem ser ligados até um eleitor individual. Essa é a essência de uma assinatura cega.

Em termos simples, o e-cash de Chaum se utiliza de assinaturas cegas como se segue: em um banco que lida com dinheiro eletrônico, você tem uma conta com $20 à qual uma senha dá acesso. Para sacar e-cash em quantias de $1 cada, você usa um software para gerar 20 números únicos e aleatórios de tamanho suficiente para que seja altamente improvável que alguém também os produza. O problema: você precisa que o banco verifique se cada número representa $1 em valor, mas você não quer que o banco saiba qual $1 é qual porque a moeda pode ser rastreada. Se não há nada mais, o banco pode combinar dados de saída e entrada, permitindo que ele saiba onde você compra, o que você compra, seu estilo de vida e outras informações que você deseja que permaneçam privadas.

Você mantém a privacidade "cegando" cada pedido com encriptação especial. O banco então recebe uma solicitação codificada na qual assina com uma chave privada de $1; isso afirma o valor e a autenticidade. O selo do banco converte o número no equivalente a uma moeda de $1 que pode ser usada apenas por você. É anônimo; o banco sabe quantas unidades de $1 ele estampou para você, mas não pode distinguir entre essas 20 unidades ou reconhecê-las de qualquer outra unidade de $1 que já autenticou.

Para gastar o dinheiro, você revela o número. Isso resulta em uma mensagem assinada válida que pode ser verificada pela chave pública do banco. As unidades de $ 1 são armazenadas em seu computador, esperando para serem enviadas para qualquer pessoa que aceite e-cash. Para fazer isso, você envia à pessoa um número decriptado e assinado, e ela o leva ao banco. A assinatura é verificada; o número de série é registrado; o valor é resgatado. Gravar o número permite que o banco rejeite qualquer tentativa de gasto duplo. Mas o banco não pode conectar a transação à sua conta, e o destinatário de $1 não tem ideia de quem você é, a menos que você decida revelar sua identidade.

O processo é tão anônimo quanto o dinheiro. Isso contrasta fortemente com o uso de cartão de crédito online, que envolve dizer a uma empresa e a um destinatário quem você é, onde está e o que está comprando. O DigiCash também está protegido contra pessoas maliciosas que estão tentando roubar identidades. Ele tem uma vantagem extra. Porque ele é altamente divisível, ele acomoda micro pagamentos – pagamentos menores de $10, para a qual os custos de transação fazem dos

cartões de crédito virtualmente impraticáveis. O e-cash era perfeito para transferir e-nickels e e-quarters pela Internet.

A DigiCash Inc. causou um grande impacto na comunidade financeira. O primeiro banco a adotá-lo foi o Mark Twain Bank em St. Louis, Missouri, mas outros logo se seguiram. Em 1998, o e-cash estava disponível através do Deutsche Bank na Alemanha, Credit Suisse na Suíça e vários outros pontos de venda poderosos. Mas, em 1998, a DigiCash Inc. entrou com pedido de falência do Capítulo 11 e posteriormente vendeu seus ativos, incluindo as patentes.

O que aconteceu? As explicações variam e todas podem conter alguma verdade.

Em uma entrevista de 1999, Chaum afirmou que o DigiCash foi uma ideia antes de seu tempo porque o comércio eletrônico não estava firmemente estabelecido. A *Forbes* teve outra explicação: “Uma admirável moeda nova para um admirável mundo novo, com apenas um problema: Ninguém queria isso – nem bancos, nem comerciantes e, mais importante, nem consumidores. O comércio eletrônico está florescendo, mas acontece que Visa e MasterCard – não dinheiro digital – são a moeda de escolha.” A maioria dos governos estavam entre aqueles que não gostaram da moeda irrastreável porque ela poderia ser usada para sonegar impostos e cometer outros “crimes” geralmente contra o estado.

Em uma fascinante peça anônima na *Next Magazine*! foi apresentada uma teoria totalmente diferente. Os criptógrafos, explica, são geralmente paranoicos. E Chaum é um GRANDE criptógrafo. O funcionamento interno do DigiCash descrito no artigo parece uma ala psiquiátrica, não uma empresa de tecnologia. Chaum é também comparado como um homem de negócios abismal. Um exemplo:

> ING Investment Management estava interessado. Este acordo foi de cerca de vinte milhões de guilders [US $ 10 milhões de dólares na época]. Os planos estavam todos traçados. O ING Barings, juntamente com o Goldman Sachs, também levaria o DigiCash ao mercado de ações dentro de dois anos. “No dia em que estávamos prontos para assinar, David não queria”, conta Stofberg [o homem responsável pelos assuntos financeiros da DigiCash].
> “Ele era tão paranoico, que sempre achava que algo estava errado. Havia 8 pessoas do ING, incluindo o CEO, e David simplesmente se recusou a assinar”!

Uma abordagem mais interessante do que psicologizar é observar algumas das fraquezas dos sistemas de e-cash e DigiCash, que contribuíram para seu fracasso e compará-los com o sucesso do Bitcoin e da blockchain.

- Chaum acreditava em patentes e direitos autorais, ambos aplicados em seus projetos. Isso restringiu severamente o acesso e o desenvolvimento cooperativo por uma comunidade global de mentes brilhantes. Colocar uma etiqueta de preço no produto dificultou a ampla aceitação do público. Por outro lado, o Bitcoin é livre de patentes e é opensource, o que dá acesso irrestrito e permite que o desenvolvimento avance.
- O e-cash não evitou o problema de terceiras partes confiáveis porque precisava de uma assinatura cega de autorização de uma instituição financeira. Além do mais, sua crescente aliança com bancos centrais proeminentes indicava uma presença crescente de terceiras partes confiáveis. O Bitcoin peer-to-peer elimina completamente terceiras partes confiáveis devido ao fato que a aceitação pela blockchain *é* a autorização, e cada participante é um self-banker.
- O e-cash exigia um emissor centralizado, como um banco. O Bitcoin é descentralizado até o nível individual.
- O e-cash preservou o sistema bancário existente. Bitcoin torna o sistema atual irrelevante.
- E-cash era vulnerável às falhas de personalidade de um homem. A comunidade Bitcoin é assombrada por conflitos internos, mas nenhuma personalidade pode destrui-la porque ninguém é dono do sistema. Além disso, sempre é possível criar uma criptomoeda alternativa para competir com uma que seja inferior de alguma forma.
- O e-cash não foi projetado para libertação financeira. O ensaio “Untraceable Electronic Cash”, de coautoria de Chaum, afirmou: “Gerar um dinheiro eletrônico deve ser difícil para qualquer pessoa, a menos que seja feito em cooperação com o banco”. Os anarquistas e idealistas que esculpiram o Bitcoin queriam empoderar o indivíduo contra os bancos e o estado e não precisavam da permissão de ninguém para fazê-lo.

Sem dúvida que as corporações mostraram interesse imediato em e-cash. Eles só recentemente mostraram interesse no Bitcoin, que agora esperam patentear, dominar e domar para seus próprios propósitos.

E-gold: Suas lições

E-gold era um sistema de moeda de ouro digital que foi operado entre 1996 e 2009 pela Gold & Silver Reserve, Inc. Em 2000, a G&SR se reestruturou e uma nova empresa, e-gold Ltd., assumiu a administração da emissão e de transferências de e-metal. A moeda digital estava ligada ao ouro, com a unidade de conta típica sendo gramas ou onças troy. Como os primeiros certificados de ouro dos EUA, o e-gold representava unidades de ouro para as quais poderia ser resgatado sob demanda do metal armazenado.

Clientes com contas no site do e-gold também podiam fazer transferências instantâneas de metais preciosos para outras contas.
Foi um dos primeiros sistemas de pagamento a permitir trocas globais complexas fora do sistema bancário tradicional. Um crítico da moeda fiduciária e dos bancos convencionais, o cofundador e libertário Douglas Jackson tinha uma missão; ele queria forjar uma alternativa privada ao lamaçal financeiro causado pelos governos. No livro *A History of Digital Currency in the United States: New Technology in an Unregulated Market* (2016), o editor da revista *Digital Gold*, P. Carl Mullan, citou Jackson como dizendo que tal “tarefa exigia capacidade computacional em larga escala, armazenamento de dados e meios de comunicação globais seguros”. Os custos eram proibitivos, exceto para os governos nacionais. Isto é, até a Internet.

Com a Internet, o e-gold foi pioneiro em vários avanços. Em 1999, por exemplo, a empresa introduziu pagamentos móveis sem fio usando um celular habilitado para web. Isso foi sete anos antes do PayPal oferecer um serviço semelhante. Uma inovação menos louvável veio em 2000, quando a empresa exigiu que os clientes que desejassem agregar valor às suas contas tivessem uma terceira parte confiável e independente que pudesse trocar e-gold por moeda e vice-versa. Em um ano, várias dezenas de empresas e indivíduos preencheram esse nicho; uma nova indústria nasceu.

De acordo com a e-gold Ltd., o número de contas cresceu de 1 milhão em 2003 para 5 milhões em 2008. Usuários de e-gold tinham

uma variedade de motivos. Alguns eram fanáticos por ouro que acreditavam devotamente que o e-gold era superior a moeda fiduciária. Outros eram anarquistas econômicos que pensavam que o governo não tinha papel adequado para desempenhar no dinheiro. Outros ainda queriam sonegar impostos ou minimizar os riscos de crimes sem vítimas.

Muitos mais inundaram os emergentes Programas de Investimento de Alto Rendimento, alguns dos quais usavam e-gold como uma plataforma de pagamento. Esses programas ofereciam altos retornos irrealistas que só poderiam ser mantidos redirecionando a riqueza de novos investidores; os esquemas Ponzi levaram a uma corrida do ouro eletrônico a um nível internacional. Os fraudadores aproveitaram os recursos do e-gold, como o fato de que todas as transações eram finais e nunca eram estornadas. Os golpistas abriram contas de e-gold e pediram aos potenciais investidores que fizessem o mesmo. Em seguida, eles extraíram dos investidores e compradores tudo o que podiam.

A essa altura, o e-gold oferecia uma ampla gama de serviços, desde cassinos e leilões online até comércio de metais e doações para organizações sem fins lucrativos. A empresa estava repleta de possibilidades para golpistas. Infelizmente, os clientes fraudados muitas vezes não faziam distinção entre o próprio e-gold ético e os vigaristas que os roubavam com investimentos falsos ou com bens inexistentes. Alguns usuários desiludidos reclamaram com as autoridades governamentais.

Em 2007, o governo federal dos EUA acusou o e-gold de lavagem de dinheiro e violação de 18 leis dos EUA. Código §1960, o qual proíbe as empresas de transmitirem moeda sem uma licença. Muitas corretoras atreladas ao e-gold foram fechadas. A publicidade e as corretoras perturbadas causaram uma queda íngreme no número de clientes e-gold; a dificuldade de trocar e-gold por moeda fiduciária fez com que potenciais recebedores de e-gold fugissem. Muitos clientes ficaram presos com contas que não podiam liquidar.

O e-gold lutou vigorosamente contra as acusações, sem sucesso. Em Abril de 2008, o juiz em *United States of America v. E-gold, Ltd*, decidiu contra a companhia e, ao fazer isso, dramaticamente aumentou o alcance de autoridade do Departamento do Tesouro. A lei agora definia um “transmissor de dinheiro” como um negócio que transferia qualquer valor armazenado de uma pessoa para outra, mesmo que a transferência envolvesse dinheiro. Este foi um cheque em branco para processos futuros.

Os três diretores da empresa se declararam culpados e firmaram um acordo pelo qual o e-gold cumpriria os requisitos legais para um negócio de transmissão de dinheiro, incluindo ser licenciado. Jackson recebeu 300 horas de serviço comunitário, 3 anos de supervisão e uma multa de US $200. Ele poderia ter recebido 20 anos e uma multa de US $500.000. Os outros dois diretores receberam a mesma sentença, com multas mais pesadas.

Então veio uma amarga ironia. As confissões de culpa impediram os diretores de adquirir uma licença em qualquer lugar nos EUA. Isso colocou todo o e-gold em bloqueio porque devolver dinheiro aos clientes envolveria a transmissão de dinheiro sem licença, o que violava o acordo judicial. Em 2010, o governo finalmente permitiu que o e-gold devolvesse o valor monetizado de suas contas aos clientes.

A definição expandida e vaga do Tesouro de "transmissor de dinheiro" tem implicações claras para o bitcoin. O sucesso do e-gold e o processo judicial contra ele mudaram a forma como o governo lidava com os sistemas de pagamento online. Agora tinha o precedente legal para agir contra a cripto.

Os paralelos entre Bitcoin e e-gold são claros. O ouro eletrônico era altamente divisível em micro pagamentos tão pequenos quanto um décimo de milésimo de grama. Mantinha um registro aberto no qual as transações diárias eram publicadas ao vivo e de forma transparente. Assim como o bitcoin, o e-gold não era uma moeda complementar. Uma moeda complementar é aquela que não compete com uma moeda nacional; um exemplo seria dinheiro privado emitido como promoção por uma empresa para clientes, que poderia ser usado para comprar mercadorias na loja. O e-gold era intencionado como um substituto para a moeda fiduciária e para o sistema bancário, com a vantagem adicional de ser um escape contra a inflação.

As diferenças entre Bitcoin e e-gold são tão importantes quanto os paralelos.

- O e-gold incorporou o problema de terceiras partes confiáveis, como descobriram os clientes encurralados por processos judiciais. É difícil culpar o e-gold pelas circunstâncias, é claro, mas a desonestidade ou a ineficiência não são os únicos riscos de confiar aos outros o seu dinheiro. O Bitcoin elimina esse problema.

- Indiscutivelmente, o e-gold introduziu um "problema do quarto confiável" quando insistiu que os clientes usassem corretoras para converter e-gold na, e para fora da, moeda fiduciária.
- O e-gold e as casas de câmbio eram pontos de centralização e alvos fáceis para regulação ou proibição. Eles também eram pontos de estrangulamento para coletar informações do cliente. Quando o e-gold foi reestruturado em 2000, o OmniPay se formou como o sistema de câmbio da empresa. O OmniPay utilizou três métodos para verificar a identidade dos clientes: verificação postal universal; pagamento apenas por transferência bancária; e, salvaguardas para detectar pagamentos recebidos de terceiros. No acordo de apelo do e-gold anos depois, o governo quase certamente obteve acesso a essas informações. O Bitcoin peer-to-peer é pseudonímico.
- A insistência do e-gold na “associação para usar” restringiu a disseminação de seus serviços. O Bitcoin está aberto a todos.

O risco de uma corretora que necessita de confiança como a OmniPay é um aviso para os usuários de cripto. Uma corretora centralizada geralmente é o primeiro alvo da regulamentação do governo porque é visível, vulnerável e constitui um cachê de dados valiosos sobre usuários de outro modo ocultos. Os proprietários de corretoras provavelmente cumprirão as exigências do governo porque a não conformidade significa ser fechado, preso ou ambos. Em suma, a centralização incentiva até mesmo terceiros honestos a obedecerem a leis e regulamentos que prejudicam os clientes.

> Empresas como Visa, Dun and Bradstreet, Underwriter's Laboratories e assim por diante conectam estranhos desconfiados em uma rede de confiança comum. Nossa economia depende deles. Muitos países em desenvolvimento carecem desses centros de confiança e se beneficiariam muito com a integração com centros mundiais desenvolvidos como esses. Embora essas organizações geralmente tenham muitas falhas e fraquezas – as empresas de cartão de crédito, por exemplo, têm problemas crescentes com fraude, roubo de identidade e relatórios imprecisos, e a Barings recentemente faliu porque seus sistemas de controle não se adaptaram adequadamente à negociação de títulos digitais e muitas dessas instituições estarão conosco por muito tempo.
> – Nick Szabo.

A maior ameaça financeira à riqueza e à liberdade das pessoas é o sistema confiável de terceiros que não atende aos clientes, mas corre, em vez disso, para cumprir as regulamentações governamentais, como os requisitos de relatórios.

O anonimato é uma ferramenta poderosa para a privacidade, mas os indivíduos também precisam evitar os canais estatais que contrariam a confidencialidade. A coleta de dados moderna é voraz, e a fiscalização está acelerando. Se você jogar o jogo do estado ao seguir os caminhos financeiros, ele vai te dirigir para baixo porque o estado escreveu o livro de regras, e ele tem a vantagem da casa. Ele não irá jogar justo. Então não jogue. Para repetir Buckminister Fuller: "Você nunca muda as coisas ao lutar contra a realidade existente. Para mudar algo, construa um novo modelo que faça do modelo existente obsoleto". Afastar-se do estado e simplesmente viver dá à liberdade a vantagem da casa. Até recentemente, no entanto, afastar-se significava um enorme sacrifício de oportunidades econômicas e de qualidade de vida porque o estado tinha uma trava no que Nick Szabo chama de "centros de confiança".

Satoshi e Buckminister Fuller

O brilhantismo do Bitcoin: ser um novo modelo do que Fuller falou. Usuários da blockchain podem se afastar de terceiras partes confiáveis sem profundo sacrifício. A blockchain ou performa os serviços válidos de uma terceira parte confiável ou torna mais óbvia a necessidade por eles. Corretoras descentralizadas – corretoras peer-to-peer – cada vez mais providenciam serviços sofisticados tais como comprar e vender cripto como especulação.

O “White Paper” de Satoshi e o passo-a-passo do “Bitcoin Whitepaper: A Beginner's Guide” mostram como a blockchain substitui as terceiras partes confiáveis. O documento define “uma moeda eletrônica como uma cadeia de assinaturas digitais”. As moedas viajam por um registro digital distribuído, chamado blockchain, pelo qual são registradas de forma transparente, cronológica e imutável. Esses são os passos básicos na jornada de uma moeda:

1. Um indivíduo transmite uma nova transação para todos os nodes ou computadores na rede.
2. Os nodes coletam a nova transação para um bloco. Um bloco é como uma página única no registro da blockchain, ele contém informação sobre uma transferência específica, bem como está processando dados.
3. O controlador de cada node – chamado de “minerador” – performa uma proof of work para o bloco. A prova de trabalho é um cálculo de computador que é difícil de produzir em termos de poder de processamento e tempo, mas é fácil para outros verificarem.
4. Quando um node tem uma proof of work, ele transmite o bloco concluído para todos os outros nodes.
5. Os nodes aceitam o bloco somente se a transação for válida e a moeda ainda não tiver sido gasta. Timestamps exclusivos, incluídos em cada bloco, evitam gastos duplos.
6. Os nodes expressam a aceitação do bloco procedendo ao trabalho no próximo na cadeia, usando o hash do bloco previamente aceito para construir uma continuidade ininterrupta de informações. Um hash é uma função que converte uma entrada em uma string alfanumérica de tamanho fixo. Cada bloco possui um valor de hash único.

Terceiros confiáveis originalmente surgiram porque eles providenciaram funções válidas para consumidores. A função incluía verificação de uma transação, facilidade e segurança de uma transferência,

preservação da privacidade, prevenção de gastos duplos, mediação de disputas e provisão de um registro. Hoje, as terceiras partes confiáveis perverteram esses valiosos serviços aos consumidores com assaltos a eles. O Bitcoin retorna esses serviços aos indivíduos sem ataques de atendentes.

Verificação de uma transação. Uma terceira parte confiável válida autentica uma transação. Um banco pode comparar a assinatura num cheque com a que está no arquivo, ou ele pode verificar que o dinheiro não é falsificado. Esses serviços têm valor, Mas uma quantia estonteante da autenticação feita pelos bancos hoje são *des*valor para os consumidores. A exaustiva verificação da identidade de um consumidor, por exemplo, viola sua privacidade para saciar o apetite do governo por dados, o que é frequentemente usado para danificar o consumidor

A blockchain verifica transações sem se intrometer nos usuários. A transferência é autenticada, não os participantes. A transação é verificada por mineradores através de uma proof of work conduzida num bloco. Uma moeda é autenticada quando a proof of work está completa e o bloco é aceito pela blockchain. Visto que a blockchain é um registro aberto público, todos podem traçar a história de uma moeda e terem a certeza da precisão de uma transação sem saberem a identidade daqueles envolvidos. O governo pode pesquisar na blockchain, mas o registro é muito mais uma barreira do que um acréscimo na fiscalização.

Facilidade de transferência. Enquanto o comércio global galopa para frente e a internet encoraja a gratificação instantânea, a velocidade e facilidade de transferências se tornou cada vez mais importante – isto é, para o consumidor. Com um monopólio virtual sobre transferências internacionais, entretanto, os bancos definem termos que os beneficia e que prejudicam o consumidor. Bancos impõe custos diretos e indiretos. Um custo direto é a taxa associada a cada transferência, que pode ser substancial. Três custos indiretos: a conversão de moeda, se necessário; as informações pessoais necessárias; e o tempo considerável que uma transferência pode levar para ser compensada. O período de compensação é chamado de “float”. Float é o dinheiro no sistema bancário que é contado duas vezes no processo de transferir o pagamento – uma vez quando ele é depositado no banco do pagador, e uma vez quando é recebido pelo banco do pagador. Visto que o banco do pagador recebe juros sobre o dinheiro flutuando, tem havido incentivo para fazer o processo mais longo do que o necessário.

Em contraste, a blockchain não reconhece distância na transferência de riqueza ou de informações. Dois computadores na mesma casa podem estar tão próximos ou distantes um do outro (em termos de tempo de transmissão) quanto dois computadores em continentes diferentes. Os mineradores cobram uma tarifa por seu serviço, mas as tarifas são conhecidas e não têm pegadinhas ocultas. Se a tarifa de transferência de uma cripto é insatisfatória, então há muitas outras criptos para se escolher. Em contraste, tarifas bancárias tendem a ser padronizadas. A maioria das transferências ocorrem rapidamente – ao menos comparando aos bancos – e não há float aí. A blockchain não tem auto interesse ou agenda escondida.

Segurança ou transferência. Até mesmo bancos honráveis podem ser hackeados, roubados e comprometidos em suas transmissões. Embora existam muitas corretoras de cripto perdendo ou roubando a riqueza de suas contas – e esse é um problema inegável – bancos são tão vulneráveis quanto. Não há uma diferença grande entre os dois, entretanto, no que tange a segurança. Toda instituição financeira over-the-table entrega informações de clientes ao governo, que utiliza os dados para tributar, confiscar, multar e prender clientes.

A blockchain é descentralizado e resiste a ataques de hackers; não pode ser corrompida por más intenções porque é inanimada. A amplamente divulgada perda de moedas por roubo ocorre quando uma pessoa passa das transferências peer-to-peer que controla para depositar suas moedas em uma corretora, especialmente uma centralizada. A comunidade cripto precisa reduzir os riscos nessa categoria de uso das criptos. O trabalho está em andamento.

Enquanto isso, nenhuma informação pessoal é entregue ao governo. O registro é transparente para todos, incluindo ao estado, mas é relativamente fácil mascarar uma identidade e embaralhar as transferências por meio de serviços como mixers ou tumblers. A blockchain é atualmente o método mais seguro pelo qual podemos transferir fundos online. A principal ameaça à segurança é se o governo tentar controlar toda a internet. Se isso for possível e se as alternativas não surgirem rapidamente, todos os métodos de transmissão online estarão ameaçados, não apenas a criptografia.

Preservação da privacidade. O tipo de privacidade outrora notoriamente oferecido pelos bancos suíços já se foi, mesmo na Suíça. As instituições financeiras são pontos de trava nos quais os dados pessoais de um cliente são coletados e compartilhados com as autoridades. A

única privacidade verdadeira é o sigilo real com que bancos informam sobre um cliente, sem o conhecimento ou consentimento do cliente.

Manter a privacidade em uma blockchain transparente parece ser uma contradição em termos. O "Bitcoin Whitepaper A Beginner's Guide" explica o porquê não é "Com a rede peer-to-peer, a privacidade ainda pode ser alcançada mesmo que as transações sejam anunciadas. Isso é feito mantendo as chaves públicas anônimas. A rede pode ver os valores dos pagamentos sendo enviados e recebidos, mas as transações não estão vinculadas a suas identidades."

Se um usuário decidir revelar as chaves públicas, uma estratégia de privacidade comum é o pseudônimo. Uma transferência peer-to-peer não requer informações para além dos cripto endereços do remetente e do destinatário, que são gerados de forma privada pela carteira de cada participante. No entanto, quando uma pessoa se junta à blockchain, ela se torna vulnerável à análise de rede que procura padrões de transferências para montar o perfil de um usuário. É por isso que alguns usuários geram um endereço diferente para cada transação, o que cria vários pseudônimos. Satoshi explica: "Quando você gera um novo endereço bitcoin, só ocupa espaço em disco em seu próprio computador (como 500 bytes). É como gerar uma nova chave privada PGP, mas com menos uso de CPU porque é ECC. O espaço de endereçamento é efetivamente ilimitado. Não faz mal a ninguém, então gere tudo o que você quiser."

Outras práticas padrões de privacidade: crie várias carteiras para isolar uma transação ou um tipo de transação de ser associado a um padrão; encobrir um endereço IP usando uma ferramenta de anonimização como o Tor; e passe por um serviço de mixagem.

Prevenção de gastos duplos. O gasto duplo ocorre quando a mesma unidade de dinheiro é gasta em mais de uma transação, embora possa ser gasta legitimamente apenas uma vez. Satoshi descreve como os sistemas de pagamento tradicionais evitam gastos duplos: "Uma solução comum é introduzir uma autoridade central confiável, ou cunhagem, que verifica todas as transações em busca de gastos duplos. Após cada transação, a moeda deve ser devolvida à casa da moeda para emitir uma nova moeda, e apenas moedas emitidas diretamente da casa da moeda são confiáveis para não serem gastas duas vezes. O problema com esta solução é que o destino de todo o sistema monetário depende da empresa que administra a casa da moeda, com todas as transações tendo que passar por eles, assim como um banco". A solução coloca a oferta

monetária nas mãos de uma terceira parte confiável, ou mesmo de uma "quarta parte confiável", o que o torna isso uma *não*-solução.

Em teoria, a cripto é suscetível a gastos duplos. Duas transações com a mesma moeda podem ser transmitidas em rápida sucessão para que a primeira não seja registrada publicamente antes que a segunda seja enviada. A solução de Satoshi é elegantemente simples. Toda transação não é somente pública, mas também adotada por todos os participantes da rede em uma linha do tempo para que possamos assumir que o pedido da cadeia é o mesmo para todos. Cada transação é marcada temporalmente. Se uma segunda transação com a mesma moeda ocorre, então a marca temporal inicial é contada, e a última descartada.

Mediação de Disputas. O dinheiro físico tinha uma vantagem sobre outras formas de pagamento; a troca é irreversível com exceção do consenso ou através de um processo judicial. A maioria dos sistemas de pagamento online possuem processos embutidos para reverter ou contestar uma transação. O serviço aumenta as tarifas gerais do sistema de pagamento, bem como colocam um limite prático sobre o tamanho mínimo de uma transação. Também aumenta o envolvimento prático do sistema de pagamento nas transações.

As transferências de blockchain são irreversíveis. Os fundos só podem ser devolvidos em uma base ponto a ponto se o destinatário concordar em fazê-lo. Isso inutiliza a necessidade de uma tarifa e permite micro pagamentos. Se a garantia tradicional do "dinheiro de volta" é desejada, então alguns serviços providenciam garantia por uma tarifa extra.

A provisão de um registro. Instituições financeiras mantém registros, mas seus conteúdos podem ou podem não ser providenciadas ao consumidor. A interação de um banco com uma agência fiscal, por exemplo, quase certamente será escondida de um titular da conta. Isso significa que muitos registros são mantidos apenas para benefício do banco e do governo, não para o cliente.

A própria blockchain é o registro. É um registro imutável e transparente de todas as transferências ocorridas desde o bloco original Genesis. Nenhuma interação oculta pode prejudicar um usuário.

Em resumo, a cripto fornece os serviços de um terceiro honesto com vantagens adicionais.

Satoshi é um Libertário e Anarquista?

Parte de explorar a dinâmica de terceiras partes confiáveis e a importância de contorná-los é perguntar: “Por que essa tarefa foi tão importante para Satoshi?” Ele era um libertário e anarquista ou ele era politicamente neutro e simplesmente farto de bancos? Uma declaração explícita de Satoshi sobre o assunto teria sido muito útil para responder a essa pergunta. Do jeito que a situação está, no entanto, o melhor que alguém pode fazer é examinar as evidências circundantes, como suas breves declarações on-line e o Whitepaper, e especular a partir da estrutura do próprio Bitcoin.

Em 31 de outubro de 2008, Satoshi publicou" Bitcoin: A Peer-to-Peer Electronic Cash System” (o “White Paper”) na Lista de Discussão sobre Criptografia em metzdowd.com. Apresentou a tecnologia por trás do Bitcoin e o design de seu instrumento de implementação – a blockchain. A breve explicação de Satoshi é um documento tecnológico definidor do nosso século.

É ainda mais notável, portanto, que ninguém parece saber a identidade de Satoshi, se “ele” é realmente uma equipe, ou muito mais sobre ele. Claramente, ele codificou por amor à tecnologia e não por desejo de fama porque evitou os holofotes; ele também não perseguiu o status acadêmico. Como o código é de código aberto e não patenteado, a aquisição de riqueza também não era uma força motriz, embora os um milhão de bitcoins em sua conta agora constituam uma fortuna incrível. Ao contrário de May e outros antecessores, Satoshi não exibiu arrogância ou desejo de chocar; em um post, ele se desculpa e modestamente diz: “Desculpe lhes dar um balde de água fria. Escrever uma descrição dessa coisa [Bitcoin] para o público em geral é muito difícil.” Em suma, ninguém pode afirmar definitivamente os motivos de Satoshi ou seu propósito final. Pelo processo de eliminação, a motivação política torna-se mais provável. Seus atos e palavras fornecem outras razões para chegarmos a essa conclusão.

Satoshi começou a escrever o código Bitcoin em 2007. Quando o “White Paper” apareceu na lista de discussão da Cryptography em 2008, também foi disponibilizado em um site criado por Satoshi – bitcoin.org. A lista de discussão consistia em especialistas em matemática, estatística e criptografia, que imediatamente argumentaram contra a viabilidade do Bitcoin. Não será escalável, alegaram; requer muitos recursos para ser prático, argumentaram. Além disso, “maus” nodes podem controlar o poder da CPU da rede e gerar uma cadeia mais longa

do que os nodes “honestos”; maus agentes poderiam controlar a blockchain.

As pacientes respostas de Satoshi gradualmente convenceram a maior parte da lista de que o Bitcoin poderia funcionar. Enquanto isso, os desenvolvimentos no lançamento aconteceram rapidamente. Os destaques incluem:

- 3 de janeiro de 2009, o bloco Genesis é extraído.
- 9 de janeiro de 2009, a versão 0.1 do software Bitcoin é lançada no Sourceforge.
- 12 de janeiro de 2009, ocorre a primeira transação de bitcoin.
- 5 de outubro de 2009, uma taxa de câmbio de US $1 = 1.309,03 BTC é estabelecida.
- 12 de outubro de 2009, o canal #bitcoin-dev é registrado para comunidades de desenvolvimento de código aberto.
- 16 de dezembro de 2009, a versão 0.2 é lançada.
- 6 de março de 2010, dwdollar estabelece uma corretora de Bitcoin.
- 22 de maio de 2010, a primeira transação no mundo real ocorre quando uma pizza é comprada por 10.000 bitcoins.
- 7 de julho de 2010, a versão 0.3 é lançada.
- 16 de outubro de 2010, ocorre a primeira transação com bitcoin como garantia.

Em meados de 2010, Satoshi transferiu a bitcoin.org para Gavin Andresen. Andresen explica:

> Comecei a enviar código para Satoshi para melhorar o sistema principal. Com o tempo, ele confiou no meu juízo sobre o código que escrevi. E, eventualmente, ele me perguntou de forma repentina se estaria tudo bem se ele colocasse meu endereço de e-mail na página inicial do bitcoin, e eu disse que sim, sem perceber que quando ele colocou meu endereço de e-mail lá, ele tirou o dele. Eu era a pessoa que todos enviavam e-mails quando queriam saber sobre bitcoin. Satoshi começou a recuar como líder do projeto e a me empurrar para frente.

Em 2010, Satoshi ficou em silêncio. Mais uma vez, fica claro que ele não escreveu pela fama.

O lançamento sistemático e meticuloso do bitcoin, bem como a estrutura elegante da blockchain, reflete um homem que pensa as situações em detalhes e entende suas implicações. Satoshi compreendeu o impacto político de seu sistema revolucionário, mas fez poucos comentários sobre o assunto.

Evidência das motivações políticas de Satoshi

Grande debate gira em torno da política de Satoshi com muitas pessoas projetando suas próprias atitudes em relação ao Bitcoin para ele. Mas todas as indicações do mundo real apontam para Satoshi ser um libertário, um anarquista ou ambos. As evidências das crenças políticas de Satoshi remontam ao bloco Genesis – o primeiro elo na blockchain. Ele contém a seguinte mensagem: "A Times de 03/Jan/2009: Chancellor à beira do segundo resgate aos bancos". A mensagem é uma manchete da primeira página do jornal britânico *The Times* de Londres. 3 de janeiro de 2009 é o aniversário do blockchain – a revelação do presente de Satoshi para o mundo. Por que ele escolheu anunciá-lo com essas palavras específicas?

Algumas pessoas pensam que o texto foi uma escolha aleatória da edição de 3 de janeiro do *Times*, e foi inserido com o único propósito de comprovar a data. Eles afirmam que a mensagem poderia facilmente ter sido "Dez profissionais do sexo presos em Sting". Esta afirmação desafia sua credibilidade. Satoshi era um programador metódico que ia diretamente ao cerne dos assuntos sem frivolidade, capricho ou apartes. Ele lançou o que ele deve ter sabido ser uma obra-prima de codificação, e não é plausível que ele tenha colocado uma mensagem aleatória no bloco Gênesis. O próprio fato de que o primeiro bloco é chamado de "Gênesis" – provavelmente uma referência ao primeiro livro da Bíblia em que Deus cria o mundo – mostra o significado que Satoshi deu ao evento.

Um cenário muito diferente é altamente provável. Satoshi está sentado em seu computador, preparando-se para lançar o primeiro bloco para o mundo como uma semente ao vento. Ele conhece seu poder e quer que as pessoas conheçam seu propósito sem ter que abrir sua concha de anonimato. Ele acabou de ler o jornal da manhã com seus rela-

tórios contínuos de torpeza financeira em que as elites políticas e financeiras agiram apenas em benefício próprio às custas dos pagadores de impostos. Uma manchete fornece o trecho perfeito sobre as duas agências mais responsáveis pelo estupro econômico dos pagamentos de impostos – o governo e o sistema bancário. As oito palavras também capturam o conluio entre eles. Satoshi digita cuidadosamente: "Chancellor à beira do segundo resgate aos bancos", e incorpora essa mensagem no Genesis de uma dinâmica que ele acredita que pode mudar o mundo. A intenção é anti-chancellor, anti-banco e anti-resgate. Desde o primeiro piscar do blockchain, ele declara que o poder do dinheiro está sendo devolvido às pessoas.

Evidências a partir do "White Paper"

Outro ponto de debate sobre as intenções políticas de Satoshi gira em torno do tom neutro do "Whitepaper". O documento ainda afirma que um sistema de instituições financeiras terceirizadas confiáveis "funciona bem o suficiente para a maioria das transações". Apenas objeções práticas ao sistema existente são delineadas nele. Em suma, o "Whitepaper" não parece um manifesto político.

Nem deveria. Um whitepaper é técnico. É uma explicação oficial de uma ideia ou experimento e de seus resultados ou conclusões, que é apresentada para revisão a especialistas na mesma área. Seu objetivo é expor um conceito, resolver um problema ou revelar uma descoberta. A ideologia não tem lugar. Além disso, a lista na qual Satoshi postou o "White Paper" era composta por especialistas em matemática, estatística e criptografia que queriam os fatos técnicos simples, não a política que os cercava. Os membros, sem dúvida, tinham uma variedade de pontos de vista políticos, e poderiam muito bem ter tropeçado em alguns com os quais discordavam. A Lista não era o momento, não era o lugar para declarar motivos ou crenças políticas.

No entanto, uma referência política está em posição de destaque. Nota de Rodapé [1] lê, "W. Dai, 'b-money', http://www.weidai.com/bmoney.txt, 1998." Este é o aceno de agradecimento de Satoshi à proposta de b-money de 1998 desenvolvida pelo famoso cypherpunk Wei Dai, com quem Satoshi teve uma troca de e-mails. A proposta de Dai é amplamente vista como uma precursora do "White Paper", com algumas pessoas acreditando que Dai é Satoshi. Em 22 de Agosto de

2007, Satoshi enviou um e-mail para Dai para o informar, “Estou ficando pronto para lançar um documento que expande suas ideias em um sistema operacional completo”. O fato de os pontos de vista de Dai serem um trampolim para o “White Paper” faz com que valha a pena examiná-los.

A proposta do b-money de Dai começa:

> Sou fascinado pela criptoanarquia de Tim May. Ao contrário das comunidades tradicionalmente associadas à palavra “anarquia”, em uma criptoanarquia o governo não é destruído temporariamente, mas permanentemente proibido e permanentemente desnecessário. É uma comunidade onde a ameaça de violência é impotente porque a violência é impossível, e a violência é impossível porque seus participantes não podem ser vinculados a seus nomes verdadeiros ou locais físicos." A proposta conclui: “O protocolo proposto neste artigo permite que entidades pseudônimas não rastreáveis cooperem umas com as outras de forma mais eficiente, fornecendo-lhes um meio de troca e um método de execução de contratos. Espero que este seja um passo para tornar a criptoanarquia uma possibilidade prática e teórica.

Também é razoável examinar os recursos que Satoshi escolheu incorporar no Bitcoin como um reflexo de sua política. Os recursos incluem

- Descentralização Radical. A primeira linha do resumo do “White Paper” afirma, “uma versão puramente peer-to-peer de dinheiro eletrônico poderia permitir pagamentos online serem enviados diretamente de uma parte para outra sem passar por uma instituição financeira”. Sem líderes, sem burocracia, sem posição de poder além do que o indivíduo exerce sobre si mesmo.
- Privacidade. A Seção 10 do “White Paper” é intitulada “Privacidade”. Ainda que não perfeito, o anonimato buscado e oferecido pelo Bitcoin é muito superior àquele de outras formas de pagamento online. A Seção 10 termina com uma advertência e, talvez, uma indicação de uma melhoria que Satoshi estava planejando

fazer para a Blockchain. "Como um firewall adicional, um novo par de chaves deveria ser usado para cada transação para impedi-las de serem ligadas a um dono comum. Algumas ligações são ainda inevitáveis com transações multi-entradas, as quais necessariamente revelam que suas entradas eram possuídas pelo mesmo dono. O risco é que, se o proprietário de uma chave for revelado, a vinculação poderá revelar outras transações que pertenciam ao mesmo proprietário."

- Pró-capitalismo. O "White Paper" enfatiza as vantagens do Bitcoin para o comércio e para os comerciantes como um sistema de pagamento de empresas livres. Ele afirma: "Com a possibilidade de reversão [que o Bitcoin não acomoda], há a necessidade da confiança se espalhar. Os comerciantes devem ser cautelosos com seus clientes, incomodando-os por mais informações do que eles precisariam". É difícil imaginar um socialista tendo essa percepção ou se importando com os comerciantes.
- Anti-bancos. Todo o propósito do Bitcoin consiste em "pagamentos online […] sem passar por uma instituição financeira." No nono fórum PGP, Satoshi explicou: "A raiz do problema com a moeda convencional é toda a confiança necessária para fazê-la funcionar. O banco central deve ser confiável para não desvalorizar a moeda, mas a história das moedas fiduciárias está cheia de violações dessa confiança. Os bancos devem ser confiáveis para manter nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito com meramente uma fração de reserva. Temos que confiar neles nossa privacidade, confiar neles para não deixar ladrões de identidade drenarem nossas contas."
- Antigoverno. Embora o governo não seja mencionado no "White Paper", o Bitcoin é um ataque direto a uma função estatal supostamente vital – o setor bancário. A mensagem no bloco do Genesis foi um tapa no Chancellor tanto quanto no resgate a bancos.
- Anti-inflação. A seção 6 do "White Paper", intitulada "Incentive", afirma que "uma vez que um número predeterminado de moedas tenha entrado em circulação, o incentivo pode fazer a transição inteiramente para taxas de transação e ser completamente livre de inflação". O número predeterminado é de 21 milhões de moedas, cada uma divisível até uma pequena fração de uma moeda inteira.

As características anteriores se aproximam de uma declaração de anarquismo econômico. Um artigo do *CoinJournal* intitulado “Op-Ed: Satoshi Nakamoto is Clearly an Anarchist” refere-se a uma apresentação de 2014 de Daniel Krawisz do Satoshi Nakamoto Institute. Krawisz afirma: “Alguém que promove bitcoin e que não é anarquista é um criptoanarquista porque o bitcoin é inerentemente anarquista.”

Evidência a partir de postagens e associações pessoais

As postagens menos formais de Satoshi em fóruns são mais uma evidência de sua política. Novamente, as observações são antibancárias e antigovernamentais, enquanto reconhecem abertamente o apelo do Bitcoin aos libertários.

- Anti-bancos. Novamente, Satoshi escreve: “Os bancos devem ser confiáveis para manter nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito com meramente uma fração em reserva.”
- Antigoverno: Quando um usuário se opõe ao Bitcoin, dizendo: “Você não encontrará uma solução para os problemas políticos na criptografia”, Satoshi responde: “Sim, mas podemos vencer uma grande batalha na corrida armamentista e ganhar um novo território de liberdade por vários anos. Os governos são bons em cortar as cabeças de redes controladas centralmente como o Napster, mas redes P2P puras como Gnutella e Tor parecem estar se mantendo.”
- Pró-liberdade. “[Bitcoin é] muito atraente para o ponto de vista libertário se pudermos explicá-lo adequadamente. Eu sou melhor com código do que com palavras”. Além disso, a postagem de Satoshi no fórum bitcointalk, O Bitcoin NÃO viola o Teorema da Regressão de Mises, indica sua familiaridade com Mises, e o tópico em si discute o livro-assinatura de Rothbard *Homem, Economia e Estado*.

Associações pessoais são outro indicador de crenças pessoais. O principal entre os associados de Satoshi era o falecido Hal Finney. Desenvolvedor da PGP Corporation, Finney foi o primeiro destinatário de uma transação de bitcoin, que Satoshi enviou a ele em 12 de janeiro de

2009. Finney obviamente cooperou de perto com Satoshi – alguns acreditam que *ele* era Satoshi – o que torna as opiniões políticas de Finney relevantes. No início dos anos 1990, Finney contribuiu regularmente para o listserv dos cypherpunks. Satoshi também postou um link para seu “White Paper” no site cypherpunk da P2P Foundation, onde ele era um membro da lista. Em um post, Finney afirma, “Naturalmente, na sociedade de hoje, com o poder alocado de forma tão desproporcional, essas ideias [criptografia] são uma ameaça para grandes organizações. O poder sendo balanceado significaria uma perda líquida de poder para eles. Portanto, nenhuma instituição vai pegar e defender as ideias de Chaum. Terá que ser uma atividade de base, na qual os indivíduos primeiro aprendam quanto poder eles podem ter e depois o exijam.”

Martti Malmi fornece outra pista. Malmi era um estudante da Universidade de Tecnologia de Helsinki, que se tornou um entusiasta do Bitcoin. O livro de Nathaniel Popper *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* descreve a jornada de Malmi. Postando no fórum anti-state.org, que explorou o anarquismo de livre mercado, Malmi escreve sobre o Bitcoin: “Estou realmente empolgado com a ideia de algo prático que possa realmente nos aproximar da liberdade em nossa vida. :-)”. Em um e-mail a Satoshi, Malmi incluiu um link para esse post.

Satoshi responde, “Seu entendimento do Bitcoin está certíssimo.”

Novamente, Satoshi percebeu totalmente o quão revolucionário seu sistema seria. Quando o Wikileaks permitiu doações de bitcoin como um modo de desviar de um bloqueio financeiro, o Bitcoin foi propulsionado a um novo nível de atenção e popularidade. Um chocado Satoshi postou: “Teria sido bom chamar essa atenção em qualquer outro contexto. O WikiLeaks chutou a colmeia das vespas, e o enxame veio em direção a nós.” Ele pediu ao Wikileaks que não destacasse o Bitcoin porque o projeto era jovem o suficiente para ser destruído pelo governo. De fato, a decisão de Satoshi de permanecer anônimo aponta para sua compreensão do perigo envolvido com o Bitcoin. Afinal, os criadores anteriores de dinheiro digital foram processados com destaque, e Satoshi deve ter observado de perto como os processos se desenrolaram.

O argumento anterior não é uma prova definitiva de que Satoshi era um libertário ou um anarquista, mas chega perto disso. “Libertário, anarquista ou ambos” tornam-se a resposta mais plausível *de longe* à pergunta sobre suas crenças políticas.

Evidência do ambiente de Satoshi

A atmosfera político-econômica da qual o Bitcoin emergiu fornece mais uma indicação das crenças de Satoshi. A codificação do Bitcoin começou em 2007, e é improvável que o momento seja uma coincidência. A crise financeira de 2007-2008 foi considerada a pior desde a Grande Depressão da década de 1930. Foi causado em grande parte pelas terceiras partes confiáveis que Satoshi mais se opunha: governos e bancos.

O que aconteceu? Em termos simplistas, a indústria de empréstimos imobiliários de alto risco entrou em colapso e provocou a crise. Um empréstimo imobiliário de alto risco é normalmente emitido para um mutuário com crédito ruim que apresenta um alto risco de inadimplência. Para compensar o credor por esse risco, o mutuário paga uma alta taxa de juros. Os empréstimos imobiliários de alto risco tornaram-se cada vez mais comuns no período anterior a 2007 por várias razões. Um foi o uso de software de subscrição automatizado que acelerou o processo de empréstimo, mas ignorou a revisão padrão de dados e documentos. Em suma, as instituições de crédito não autenticaram a elegibilidade do mutuário. Os preços da habitação dispararam devido a uma enxurrada de crédito artificialmente solto. Atingindo o pico em 2006, os preços iniciaram uma espiral descendente que durou anos e causou execuções massivas tanto nos EUA quanto internacionalmente.

A alta taxa de inadimplência levou a uma desvalorização dos instrumentos financeiros, o que ameaçou o colapso do confiável sistema de terceiros – também conhecido como sistema financeiro. O Estado não iria e não poderia permitir que isso acontecesse; o sistema financeiro era seu braço direito. Em 7 de setembro de 2008, o governo federal dos EUA assumiu as responsabilidades dos extremamente abalados Freddie Mac e Fannie Mae. Outros resgates se seguiram. Em 3 de outubro, a Lei de Estabilização Econômica de Emergência de 2008 autorizou gastos de até US$ 700 bilhões para comprar ativos em dificuldades e financiar instituições financeiras, inclusive estrangeiras. O custo de salvar a hierarquia de terceiras partes confiáveis foi repassado aos pagadores de impostos, é claro.

Satoshi observou os resgates se desenrolarem, como atesta a mensagem de bloqueio do Genesis. A pilhagem de fundos de impostos para enriquecer a elite, enquanto as pessoas comuns perderam suas casas, deve ter parecido um pesadelo de terceiras partes confiáveis.

Outra coisa ocorreu em 2007. O governo federal dos EUA acusou os chefes da e-gold, Inc. de lavagem de dinheiro e transmissão de dinheiro sem licença. Os donos do e-gold foram julgados e condenados; a empresa arruinada foi forçada a fechar suas portas eletrônicas. Satoshi deve ter visto essa situação bem de perto. Ele aprendeu disso. O anonimato era segurança.

Legado de Satoshi

Satoshi produziu uma tecnologia elegante e original que rivaliza com a impressora de Gutenberg em sua importância para o progresso humano porque permite fácil liberdade econômica em nível individual.

O paralelo merece expansão. Embora sua impressora não tenha sido a primeira, Johannes Gutenberg foi pioneiro em inovações criativas que tiveram um impacto semelhante à criação de Satoshi. Ele substituiu as tintas à base de água de curta duração por uma durável à base de óleo, por exemplo. Mais importante ainda, ele usou uma forte liga para criar cerca de 300 bits de tipos separados que poderiam ser rapidamente montados em modelos uniformes e desmontados. As impressoras anteriores usavam pedaços de madeira frágeis ou esculpiam as letras de cada página em um bloco de madeira que era pintado. As inovações transformaram a imprensa de uma ferramenta das classes de elite – a corte, o clero – em uma ferramenta do povo. Gutenberg abriu um mundo de informações e ideias para pessoas comuns que não precisavam mais confiar nas autoridades para sua versão da verdade. A imprensa descentralizou o conhecimento nas mãos do homem comum, e conhecimento é poder. Isso tornou a imprensa não apenas uma maravilha técnica, mas também um agente de mudança e revolução social.

Os que estão no poder teriam evitado a mudança, se pudessem, suprimindo a enxurrada de opiniões e ideias. Um público iletrado, não informado, é mais fácil de controlar. Um público letrado e informado encoraja a ascensão do populismo e de reformadores que ameaçam o status quo. Preservar um status quo favorável ao poder é a principal razão pela qual a censura estatal existia então e agora, sendo o controle da imprensa um fator essencial. Infelizmente para os poderosos, a literatura aumentou e mais pessoas puderam julgar por si mesmas quais crenças religiosas e políticas ressoavam dentro delas como reais.

Um exemplo de convulsão social: sem a imprensa de Gutenberg, a Reforma Protestante provavelmente não teria ocorrido, ou teria sido

muito limitada em escopo. Martinho Lutero lançou a Reforma em 1517 pregando suas noventa e cinco teses na porta de uma igreja alemã. O documento foi rapidamente traduzido do latim para o alemão, depois copiado e reimpresso; no jargão de hoje, tornou-se viral. Como homem, Lutero só podia alcançar aquelas pessoas dentro do alcance de sua voz e caneta. Como um autor produzido em massa, Lutero espalhou ideias por toda a Europa em poucos meses. Em três anos, centenas de milhares de cópias de suas Teses foram produzidas em centenas de prensas tipográficas. A Igreja Católica respondeu excomungando Lutero, levando-o a fugir e a se esconder. As ideias, entretanto, não respondem a ameaças de fogo do inferno, nem fogem.

A imprensa de Gutenberg provocou movimentos e revoluções. Mas a imprensa em si não era ideológica, pois qualquer ideia podia ser montada em moldes e impressa em massa: Catolicismo ou Protestantismo, individualismo ou socialismo, Karl Marx ou Ayn Rand. A máquina ela mesma era neutra. A prensa teve fortes implicações ideológicas, com certeza, porque deu poder ao indivíduo e às massas. Em outras palavras ela era uma forma populista. Mas as autoridades também usaram a nova tecnologia para seus próprios fins estatistas. Por mais magnífica que fosse a imprensa, era uma ferramenta para o bem ou para o mal, dependendo da finalidade do usuário individual.

O mesmo pode ser dito da cripto. Seu empoderamento do indivíduo é um ato profundamente político. Mas esse empoderamento faz todos serem mais livres para escolher quaisquer ideologias que eles queiram. A própria cripto não possui posição ideológica estabelecida. É por isso que individualistas, anarquistas, socialistas, estatistas e entre outros podem usar a blockchain como um modo de perseguir seus fins, independentemente de quais fins esses possam ser. Amir Taaki, um desenvolvedor da Darkmarket? Openbazaar e da Dark Wallet, é um anarquista de esquerda agressivo que passou um tempo em Rojava [Kurdistão Sírio], ajudando a fundar uma República Popular através da introdução do Bitcoin. Rojava estava "sob embargo, então não havia maneira de mover dinheiro para dentro ou para fora", ele explica. "Então temos realmente de criar nossas próprias economias em bitcoin. Agora temos uma ferramenta tecnológica para as pessoas livremente se organizarem fora [do] sistema do estado. Porque é uma moeda não controlada por bancos centrais."

O Bitcoin pode atingir uma diversidade galopante de objetivos. Essa é uma grande força. A prensa de Gutenberg providenciou informação e perspectivas que permitiram as pessoas escolherem religião e políticas *por elas mesmas*. A cripto dá às pessoas o controle de seu próprio futuro econômico que lhes permite escolher seus próprios estilos de vida e compromissos. Parte do que faz a Revolução Satoshi brilhar é que ela é profundamente política ao empoderar o indivíduo, mas não exige uma posição ideológica. Ou seja, não diz aos indivíduos empoderados o que eles devem escolher ou como eles podem usar seu próprio poder. A maioria das pessoas veem pouca diferença entre o político e o ideológico. Geralmente não há. Mas às vezes a política e a ideologia são distintas.

O Bitcoin é político no mesmo sentido em que a prensa de Gutemberg. Ela descentraliza o controle até o nível do indivíduo – a cripto é puro empoderamento – mas ela não dita o que indivíduos fazem com seu autocontrole. Isso seria uma contradição em termos. Ainda sim é isso que o estado faz quando ele tenta controlar a cripto; ele tenta vincular uma contradição em termos com a sociedade. O estado toma uma dinâmica inerentemente descentralizada e individualista e tenta centralizá-la ao torná-la um braço do governo. As boas notícias: as tentativas do estado parecem fadadas ao fracasso. A má notícia: o estado continuará tentando.

O Governo Leva a Cripto a Sério

O melhor status para se ter vis-à-vis ao estado, no final das contas, é nenhum – isto é, passar despercebido enquanto você vive sua vida em paz e em liberdade. A invisibilidade é, entretanto, um status difícil ou caro de se alcançar, e o governo pune punições rígidas àqueles que tentam sem sucesso. A cripto perdeu a invisibilidade legal que inicialmente gozou de ser arcana ou desconsiderada como uma faísca numa panela. Está sendo tomada seriamente e é "vista" pelas autoridades. Chamar a atenção do estado é provavelmente o que Satoshi quis dizer quando lamentou a proeminência que o Bitcoin alcançou por meio de sua associação com o Wikileaks. A tecnologia era jovem e estava em desenvolvimento inicial; a última coisa que precisava era ser levada a sério pelo governo. Como Satoshi comentou, "A WikiLeaks chutou o ninho de vespas, e o enxame está vindo em nossa direção."

O objetivo do enxame do estado é previsível – controle –, mas a reação das autoridades varia. Alguns políticos e burocratas percebem uma ameaça; outros vislumbram a mais nova pilhagem possível; outros ainda veem um meio de atualizar um sistema bancário central ineficiente e impopular; muitos querem usá-lo como trampolim para uma sociedade sem dinheiro que eles controlam digitalmente. Quaisquer que sejam as diferenças de perspectiva, no entanto, a mesma conclusão é alcançada: a criptografia precisa estar sob sua autoridade centralizada.

Uma estratégia do estado para controlar a cripto

Uma estratégia popular de estado para dominar cripto é reclassificá-lo como dinheiro e aplicar as mesmas leis rigorosas que cobrem a fiat. Um projeto de lei atualmente parado no Senado dos Estados Unidos incorpora aspectos comuns dessa tática, que está longe de se limitar às costas americanas. Examinar o projeto de lei é uma maneira de entender como essa estratégia provavelmente funcionará e como o processo destruiria as criptomoedas, caso bem-sucedido.

Na terça-feira, 28 de novembro de 2017, o Projeto de lei 1241 do Senado foi ouvido pela Comissão de Justiça do Congresso. O projeto de lei foi discutido no comitê onde ele permanece. É um alarme soando à noite.

Alguns entusiastas das criptos vão aplaudir esse desenvolvimento porque acreditam que a regulamentação significa que a cripto está se tornando mainstream e alcançando uma respeitabilidade que traz mais lucro. Alguns entre aqueles que aplaudem querem se beneficiar de licenças (aprovações governamentais), o que poderia eliminar os concorrentes de livre mercado. Outros fanáticos por criptomoedas apenas irão cruzar os braços porque pensam que as criptomoedas de livre mercado não podem ser controladas e os esforços estatistas falharão. Os indiferentes podem estar corretos – espero que estejam –, mas vidas podem ser destruídas pela tentativa do estado de dominar, e a destruição de pessoas boas é um assunto de não se cruzar os braços. A abordagem prudente à intrusão do estado não é nem o aplauso, nem a indiferença, mas preparação. O governo está chegando e ele quer mais que dinheiro. Ele quer dar exemplos contundentes de usuários de cripto para dissuadir outros de buscar a liberdade financeira.

A "Lei de Combate à Lavagem de Dinheiro, Financiamento do Terrorismo e Falsificação" (S.1241) é um projeto de lei contra a lavagem de dinheiro que regula a criptomoeda a nível federal. Isso significa que haveria uma uniformidade no status legal e no tratamento das criptomoedas em toda a América.

Novamente, alguns entusiastas de criptomoedas aplaudirão esse movimento por fornecer clareza à situação. Essa é uma resposta enganosa em vários níveis. Por um lado, controle não é clareza; é a centralização e a entrega da escolha. E a clareza não tem valor intrínseco à parte do conteúdo que está sendo esclarecido; um assassino pode ser muito claro sobre como ele pretende matar você, mas isso não é algo para comemorar ou buscar. Por outro lado, se inconsistências legais no tratamento das criptos causarem problemas, então a resposta apropriada é remover as leis, não exigir mais.

Além disso, inconsistências na lei podem ser úteis porque podem funcionar para a vantagem daqueles que buscam a liberdade. A estratégia é às vezes chamada de abordagem da "instituição paralela". Instituições paralelas como a Igreja e o Estado podem atuar como baluartes contra o poder um do outro, permitindo que os indivíduos respirem mais profundamente na divisão. O conceito de santuário da igreja estava tradicionalmente disponível para criminosos e escravos fugitivos, por exemplo, embora não fosse oferecido de forma confiável. Por outro

lado, pessoas com crenças religiosas ou políticas "erradas" às vezes podem escapar da perseguição fugindo para o santuário de uma área politicamente mais amigável.

A estratégia da instituição paralela é empregada todos os dias em todo o mundo. Na América, as pessoas se mudam de estados com altos impostos para estados com poucos ou nenhum imposto. Os ricos britânicos se mudam para paraísos fiscais. Os aficionados da maconha se mudam do Texas, com suas leis draconianas sobre drogas, para o Colorado, onde a maconha é legal. Em todo o mundo, as pessoas fogem por suas próprias razões.

A liberdade não se beneficia da homogeneização da lei governamental, mas da presença de alternativas. A federalização da lei sobre criptomoedas para eliminar a inconsistência também elimina a capacidade dos usuários de se mudarem para qualquer jurisdição estadual que seja mais favorável ao seu propósito. A federalização da lei também expande o governo para áreas que ainda não são abordadas no nível estadual; isso inclui controle de fronteira e alfândega. A consistência pode trazer clareza, mas ela não traz escolha. Outra palavra para consistência na lei é a palavra "centralização".

O que é a S.1241?

S.1241 foi introduzido no Comitê do Senado secretamente. Um bitcoiner atencioso notou que a reunião do Judiciário do Senado havia sido listada na página oficial às 10h do dia 28 – o mesmo dia da audiência – depois de ser adicionada à página da Audiência às 18h. na noite anterior. Essa manobra efetivamente impediu a cobertura da mídia, feedback do público ou protestos. Ações para controlar a cripto são prováveis de seguir esse padrão – abrupto, invisível e inesperado. A S.1241 pode ser vista como um modelo de como os governos pretendem proceder. Para onde os EUA vão, grande parte do mundo vai.

A S.1241 procura emendar o Código 31 § 5312, que trata das definições e sua aplicação a dinheiro e finanças. Parece seco, mas o impacto seria dramático. O objetivo do projeto de lei é incluir "moedas digitais" na definição de "instrumentos monetários" e incluir "qualquer corretora digital ou trocador de moeda digital" na definição de "instituição financeira". $10.000 é o valor acionante da lei. Nos EUA. $10.000 aciona uma declaração pessoal na margem; é o ponto em que as instituições financeiras completam um relatório de moeda exigido

pelo estado que pode fazer com que as contas sejam congeladas ou confiscadas, independentemente de haver evidência de um crime

A S.1241 é uma corda apertada

Seção 2: "Transporte ou Transbordo de Cheques em Branco ao Portador" declara que qualquer cheque entrando ou saindo dos EUA que seja "extraído em uma conta contendo mais de US$ 10.000" e não tenha um valor em dólar especificado é "valorizado acima de US$ 10.000 para fins de relatório". Visto que a cripto pode ser difícil de se ensaiar e raramente tem um valor em dólar especificado, o "valor sem dólar" permite que os agentes alfandegários avaliem a cripto no valor registrável.

Seção 3: "Aumentar as penalidades para o contrabando de dinheiro a granel" aborda a ocultação de $10.000 ou mais em moeda ou instrumentos monetários ao cruzar a fronteira. A pena máxima é de dez anos de prisão com multas aumentando em um valor não especificado. Quando o estado pune uma pequena ofensa de maneira draconiana, isso significa que as autoridades não têm outra solução para a situação senão o cano de um fuzil.

Seção 4: A "Seção 1957 Violação Envolvendo Fundos Combinados e Transações Agregadas" trata da "transferência de produtos criminais [...] Sem a necessidade de demonstrar" intenção criminosa. Duas brechas existentes seriam fechadas. 1) $10.000 em fundos nos quais dinheiro supostamente sujo é misturado com dinheiro limpo tornam-se $10.000 de dinheiro sujo. 2) Uma série de transações abaixo de $10.000 que estão "intimamente relacionadas no tempo, a identidade das partes, a natureza das transações ou a maneira como são conduzidas" atendem coletivamente ao limite de $10.000. O dinheiro legal que está na presença de dinheiro "criminoso" é culpado por cumplicidade, permitindo que os funcionários confisquem tudo. Cripto não declarada ou declarada incorretamente torna toda a riqueza – seja cripto ou não – um alvo fácil.

Seção 5: "Acusação de lavagem de dinheiro como um curso de conduta" simplifica o processo de acusação de uma pessoa por lavagem de dinheiro e inclui "conspirações para violar [...] [a] proibição das empresas que transmitem dinheiro não licenciado são rotuladas enquanto conspirações de lavagem de dinheiro". Planos de transmissão de cripto podem ser punidos como se o ato tivesse ocorrido. Não está claro se os

co-conspiradores também serão acusados ou terão seu dinheiro confiscado.

Seção 6: “Empresas de serviços financeiros ilegais” torna crime para empresas não registradas enviar “receitas para o exterior”. O desconhecimento da necessidade de registro não é defesa. O termo “negócio de transmissão de dinheiro” é substituído por “negócio de serviços monetários” para incluir “entidades [...] como caixas de cheques” que “não transmitem dinheiro”. As penalidades e multas aumentam.

Seção 7: “Lavagem de dinheiro oculta” aplica-se a “entregadores ou mulas”. A Suprema Corte decidiu no passado que um réu precisa saber que o transporte de fundos é clandestino e porque os fundos estão sendo “transportados” para que um entregador seja culpado de um crime. Esses requisitos são diluídos ou eliminados. Novamente, ignorância não é uma defesa.

Seção 8 “Congelamento de contas bancárias de pessoas presas pela movimentação de dinheiro através das fronteiras internacionais”. Uma retenção de 30 dias é instituída nas contas dos acusados e pode ser estendida “por uma boa causa”. Isso parece se aplicar ao valor total de uma conta.

Seção 9: “Proibir a lavagem de dinheiro por meio de Hawalas, outros sistemas informais de transferência de valor e transações estreitamente relacionadas” redefine o que constitui um crime de lavagem de dinheiro quando envolve “um conjunto de transações paralelas ou dependentes”. Todos seriam considerados “um único plano ou arranjo”, o que poderia levar a transação coletiva a níveis passíveis de ação judicial.

Seção 10: “Restaurar a autoridade de escutas telefônicas para certas infrações de lavagem de dinheiro e falsificação” permite que o estado monitore as pessoas suspeitas de atividade criminosa.

Seção 11: “Aplicando o Estatuto Internacional de Lavagem de Dinheiro à Evasão Fiscal” define o uso de contas estrangeiras para sonegação de impostos como lavagem de dinheiro. Como a cripto flui tão facilmente através das fronteiras, os usuários tendem a frequentar corretoras “estrangeiras” – uma prática que pode ser rotulada de “evasão fiscal”, a menos que se prove o contrário.

Seção 12: “Conduta em auxílio à falsificação” inclui o uso de novas tecnologias, “materiais, ferramentas ou maquinário”. Esta disposição visa especificamente a criptomoeda, o dinheiro digital e as ferramentas que fornecem privacidade a eles.

Seção 13: "Dispositivos de acesso pré-pago, cartões de valor armazenado, moedas digitais e outros instrumentos semelhantes" altera a lei atual para incluir explicitamente "qualquer corretora digital ou tumbler de moeda digital", bem como qualquer "emissor, resgatador ou caixa" de uma "moeda digital". Os fundos armazenados em formato digital estão explicitamente sujeitos a requisitos de relatórios de lavagem de dinheiro.

Seção 14: "Intimações Administrativas para Casos de Lavagem de Dinheiro" expande a disponibilidade e facilidade de intimações administrativas.

Seção 15: "Obtenção de Registros Bancários Estrangeiros de Bancos com os EUA. Contas Correspondentes" fortalece "essa ferramenta de investigação existente". Bancos estrangeiros podem ser intimados para registros relacionados a qualquer "ação de confisco civil" e podem ser punidos por descumprimento. Relembre-se: A S.1241 inclui "qualquer cambiador digital ou tumbler moeda digital" na definição de "instituição financeira", o que deixa as moedas estrangeiras vulneráveis a intimações.

Seção 16: "Danger Pay Allowance" fornece compensação especial para uma ampla gama de agências de aplicação da lei. Não está claro o que constitui "perigo", mas, presumivelmente, as agências terão interesse em definir situações de uma maneira que atraia mais financiamento.

Seção 17: "Esclarecimento da Autoridade do Serviço Secreto para Investigar Lavagem de Dinheiro" expande a autoridade policial.

Seção 18: A "Proibição de Ocultação de Titularidade de Conta" torna crime que uma pessoa "oculte, falsifique ou deturpe conscientemente, de ou para uma instituição financeira" sua identidade ou "fato relativo à propriedade ou controle de uma conta ou ativos mantidos em uma conta." Isso é particularmente relevante para usuários de cripto que rotineiramente empregam anonimato ou pseudonimato. Torna-se um crime não revelar identidades ou transferências específicas na blockchain.

Seção 19: A "Proibição de Ocultação de Fonte de Ativos em Transações Monetárias" permite que o governo busque ativos mesmo que a pessoa não seja acusada de um crime. Em vez disso, seu dinheiro pode ser confiscado simplesmente porque sua fonte não é declarada ou não é manifesta.

O advogado Ballard Spahr explica: “Se aprovado em sua forma atual, a S.1241 ironicamente levará ao único tipo de ofensa que o Congresso historicamente não tem permitido, construir um pretexto na aplicação das leis de lavagem de dinheiro – ou seja, tratar como tal a fraude fiscal “comum”, que não envolve receitas ilegais – e virar as coisas de cabeça para baixo. Ou seja, as transações que promovam um crime fiscal, desde que envolvam uma transação transfronteiriça, serão o único tipo de transação que pode constituir um crime de lavagem de capitais quando os rendimentos representarem fundos inteiramente legais.”

Aqueles que desejam se preparar contra a repressão vindoura devem estudar a S.1241.

Protegendo as pessoas de sua liberdade

Lavagem de dinheiro e evasão fiscal são duas justificativas que o estado proclama quando tenta controlar as criptos. Indiscutivelmente, essas justificativas amplas e vagas não são vistas com simpatia geral, porque muitas vezes parecem um flagrante roubo monetário.

Outras justificativas são mais bem-sucedidas. A comunidade cripto, argumenta o governo, está repleta de traficantes de drogas, chantagistas, traficantes de sexo, produtores de pornografia infantil, traficantes de armas e outros malfeitores. O estado aponta a “dark web” como prova dessa perfídia. Esta é a parte da web que é acessada apenas por software especial, permitindo que os usuários permaneçam anônimos ou não rastreáveis. Diz-se que o controle de criptomoedas é necessário para proteger as pessoas do crime na dark web. Ao fazê-lo, o estado argumenta que está protegendo usuários de drogas vulneráveis, mulheres e crianças exploradas, vítimas de armas, pagadores de impostos obedientes, cidadãos cumpridores da lei e uma lista de outras “vítimas” dos bandidos monetários.

Existem inúmeras maneiras de refutar essa afirmação, incluindo o fato de que ela é totalmente falsa. Alguns usuários de cripto são, sem dúvida, criminosos violentos; o mesmo acontece com algumas pessoas que usam dinheiro e cartões de crédito. Criptos são moedas e métodos de pagamento. Como qualquer outra coisa útil na vida, é uma ferramenta que pode ser empregada para bons ou maus propósitos. Mas a esmagadora maioria das pessoas com cripto ou com dinheiro são seres humanos pacíficos que estão sendo criminalizados por preferir um método de pagamento em detrimento de outro. A justificativa para isso se

resume à alegação de que suas escolhas econômicas são perigosas para o bem-estar público.

Reprimir práticas econômicas supostamente exploradoras, mas não violentas, é uma tremenda violação dos direitos das pessoas vulneráveis; não os protege. Eu sei. Minha vida poderia ter sido arruinada por uma medida destinada a evitar a assim chamada forma de exploração econômica que repugna à maioria das pessoas – o trabalho infantil. Aos 16 anos, fugi de casa e morei na rua o menor tempo que pude. Recusei-me a ir para um abrigo ou procurar ajuda do governo pelo mesmo motivo que muitos adolescentes fugitivos; quando os adolescentes preferem o relento à casa, significa que os adultos os traíram. A única segurança é cuidar de si mesmo.

Eu tive mais sorte do que muitos. Eu mal tinha 16 anos, mas isso significava que eu poderia trabalhar legalmente. Eu poderia ficar atrás do balcão quente em um restaurante de fast food ou, no meu caso, poderia sentar-me no escritório de uma loja de móveis de propriedade familiar, onde eu fazia anos de papelada durante o dia e dormia em um sofá no andar de baixo durante a noite. O dono me pagava um salário-mínimo e me dava um lugar seguro para dormir. Como resultado, trabalhei muito mais do que as oito horas diárias pelas quais fui paga. Economizei o suficiente para me mudar para uma pensão e, quando passei para um trabalho de arquivamento em um banco, tive uma referência. Meu futuro dependia de ter essas oportunidades.

E se eu fosse um mês ou um ano mais nova do que a idade legal para trabalhar? O dono da loja não teria arriscado seu negócio me contratando. Nem deveria. Ele estava certo em insistir em inspecionar e xerocar minha identidade. antes de me oferecer o emprego; ele estava certo em esperar até me conhecer um pouco melhor para me oferecer o sofá do porão. Por que ele deveria colocar a renda e o futuro de sua família em perigo para ajudar uma estranha? E foi isso o que ele fez; ele não me explorou. Ele me *ajudou*.

Sem a capacidade de ganhar dinheiro legalmente, minha vida poderia ter acabado mal em vez de bem. Em nome do humanitarismo, a lei teria trancado minha única porta para a sociedade comum, e teria feito isso segundo seu próprio parâmetro arbitrário de justiça. Como eu teria me alimentado então? Roubo, mendicância, trabalho sexual e tráfico de drogas vêm à mente. Mas eu queria um caminho *para fora* da rua, não uma forma de fazer dela ou da prisão meu endereço permanente.

Fechar opções econômicas não violentas não protege as pessoas vulneráveis. Assim como o aumento do salário-mínimo obrigatório torna difícil encontrar emprego para quem está começando, as "proteções" econômicas impedem que as pessoas vulneráveis possam ascender. No meu caso, não poder me sustentar teria criado uma criminosa e uma vítima, diminuindo o bem público. Se houver violência envolvida em uma opção econômica, então trate a violência. Se não houver, então deixe isso sozinho. Este princípio é a maneira de ajudar a todos que querem ganhar seu próprio dinheiro e gastá-lo como bem entenderem. O estado não protege as vítimas ou a sociedade tirando opções econômicas de pessoas que não causaram danos demonstráveis, mas que por acaso se enquadram em uma categoria que é protegida ou vilipendiada.

Estranhamente, a resposta da lei a ambas as categorias é mais do mesmo: negar direitos econômicos. Como uma adolescente fugitiva, eu estava na categoria "protegida" e quase perdi meu direito de ganhar a vida. Usuários de criptomoedas pacíficos estão na categoria "injuriados", e muitos podem ser destituídos do direito de reter o dinheiro que ganharam.

Para beneficiar os vulneráveis e a sociedade, o estado não precisa fazer nada além de sair do caminho. A frase francesa "laissez faire" é mais frequentemente associada ao "capitalismo laissez-faire". Diz-se que se originou durante uma reunião de 1681 entre Jean-Baptiste Colbert, o Controlador-Geral de Finanças francês, e um grupo de empresários. Colbert perguntou como o Estado poderia ajudar os homens em seus negócios. O chefe do grupo, M. Le Gendre, teria respondido: "laissez nous faire" (deixe conosco). Deixe-nos em paz.

Uma segunda estratégia de controle: Cripto emitida pelo governo

Alguns estados planejam ou tentam emitir sua própria criptomoeda. A moeda digital emitida pelo Banco Central (CBDC) refere-se a uma criptomoeda nacional emitida por um banco central. É a contrapartida cripto de uma moeda fiduciária física, como o dólar americano ou a libra esterlina.

É também uma ironia amarga. Um pulo do gato monetário que foi projetado para minar o sistema financeiro está sendo redefinido para servir ao status quo. Pelo menos, é isso que o status quo espera que aconteça. Para ser justo, alguns líderes mundiais entendem que esse desenvolvimento não é possível. Putin de forma infame disse que uma

criptomoeda nacional não é viável porque a criptomoeda é um fenômeno internacional. Outras nações estão explorando ativamente o desenvolvimento de CBDCs, no entanto. O Japão lançou o dinheiro digital J-Coin, por exemplo. É uma moeda digital em vez de ser uma criptomoeda baseada em blockchain, mas serve ao propósito de aproximar o Japão de uma sociedade sem dinheiro vivo; torna o rastreamento de usuários de moedas digitais uma questão trivial; e permite que o estado reprima usuários de criptomoedas reais com maior facilidade e menos reação. Esses são três dos principais objetivos de uma moeda eletrônica nacional.

As CBDCs podem parecer paralelos à cripto de livre mercado, mas elas são anticripto. Considere apenas algumas das diferenças técnicas:

- Bitcoin é descentralizado; As CBDCs centralizariam todos os aspectos da moeda digital, muitas vezes nas mãos de uma agência ou sistema de agências que são fortemente regulamentadas.
- Bitcoin é peer-to-peer entre indivíduos; CBDCs seriam administradas por terceiras partes confiáveis no pior sentido desse termo.
- Bitcoin é de código aberto; Os CBDCs seriam patenteadas, proprietárias e não transparentes.
- Bitcoin é minerado; CBDCs seriam emitidas por uma autoridade central.
- Bitcoin é limitado a 21 milhões de moedas; O limite das CBDCs seria o que a autoridade desejasse.
- O Bitcoin está em uma blockchain transparente; CBDCs podem não usar uma blockchain, e provavelmente não usariam.
- Os usuários de Bitcoin possuem suas próprias chaves privadas; chaves privadas para CBDCs seriam de propriedade de uma terceira parte confiável que controlaria a riqueza.
- Bitcoin é anônimo; Os CBDCs rastreiam as identidades dos usuários e como eles gastam a moeda.
- O Bitcoin corta a conexão entre a moeda e os bancos centrais; Os CBDCs iriam cimentá-la.

As criptos de livre mercado e as CBDCs também têm objetivos antagônicos. A criptomoeda torna obsoleto o status do banco central como uma terceira parte confiável e elimina o monopólio do dinheiro. As CBDCs são a tentativa do sistema de banco central de manter seu status de terceira parte confiável e o monopólio monetário.

As criptomoedas de livre mercado e as CBDCs podem ter um objetivo em comum, no entanto: a eliminação final do fiat. Mas, novamente, as razões são antagônicas. A cripto rejeita uma moeda corrupta que rouba de pessoas honestas. As CBDCs querem resgatar o status quo em benefício das elites financeiras criando uma fiat digital.

Por que o impulso para uma sociedade sem dinheiro?

O dinheiro congelado sempre foi o inimigo de governo. Em seu artigo "Por que os governos odeiam o dinheiro", o professor de economia Joseph Salerno escreve:

> Agora, a razão dada por nossos governantes para suprimir o dinheiro é manter a sociedade a salvo de terroristas, sonegadores de impostos, lavadores de dinheiro, cartéis de drogas e outros vilões reais ou imaginários. O real objetivo da enchente de leis restringindo ou até proibindo o uso de dinheiro é forçar o povo a fazer pagamentos através do sistema financeiro. Isso permite que os governos expandam sua capacidade de espionar e acompanhar as transações financeiras mais privadas de seus cidadãos, a fim de extrair deles até o último dólar de pagamentos de impostos que eles alegam ser devidos.

O problema que as autoridades enfrentam: Quando o dinheiro sai do banco e vai para os bolsos dos indivíduos, o governo perde a noção de como é gasto. Os indivíduos podem comprar e vender com um anonimato que bloqueia a cobrança de impostos, taxas e outras receitas para o estado. O governo quer "resolver" isso. Sites de rastreamento de dinheiro podem registrar os números de série da moeda fiduciária, por exemplo, e permitir que a circulação seja monitorada, ou seja, desde que o número de série seja reinserido em todas as etapas. O sistema requer um alto grau de cooperação improvável.

O impulso em direção à moeda fiduciária rastreável inevitavelmente falhará devido à falta de cooperação. Felizmente para governos e bancos centrais, o dinheiro digital é um substituto perfeito para o dinheiro físico porque a rastreabilidade é incorporada ao projeto. Se os governos conseguirem fazer o dinheiro digital funcionar, os dinheiros

resultantes serão um pesadelo para a liberdade. Eles combinarão a eficiência das criptomoedas com o totalitarismo do governo. O problema da terceira parte confiável que o Bitcoin foi criado para eliminar estará de volta com esteroides.

A hostilidade do estado ao dinheiro fará com que algumas nações passem da moeda fiduciária física para a digital com entusiasmo. É provável que o processo se pareça com alguma versão do seguinte:

Primeiro: Um governo explora a possibilidade de dinheiro digital enquanto remove gradualmente o dinheiro físico de circulação.

Segundo: Um banco de dados para moeda digital – provavelmente não baseado em uma blockchain – é escrito em código proprietário e implementado de maneira não transparente.

Terceiro: Um dinheiro digital é emitido e vendido como uma alternativa ao dinheiro e à cripto de livre mercado. Para encorajar sua adoção, o governo regula as criptos de livre mercado que são levadas à clandestinidade ou forçadas a fugir para climas mais amigáveis.

Quarto: A tributação automática é embebida na nova moeda digital. O rastreamento absoluto de cada unidade de moeda, que está ligada a identidades reais, dá ao governo um controle sem precedentes sobre o fluxo de riqueza.

Quinto: Bancos centrais inflacionam a oferta de moeda digital à vontade, desvalorizando cada unidade em circulação. Isso inflige um imposto enorme e oculto a todos os proprietários.

A CBDC também dá ao governo maior precisão na manipulação da economia. Em um artigo intitulado “Por que os governos querem uma moeda digital emitida pelo Banco Central”, o economista austríaco Xiong Yue observa:

> [D]ado que essas moedas digitais são programáveis, o governo pode até controlar exatamente como gastar esse novo dinheiro usando scripts. Por exemplo, se o governo planeja subsidiar certas fazendas, digamos algumas fazendas de milho, para apoiar este setor da agricultura, eles podem adicionar diretamente uma certa quantia de dinheiro às carteiras de algumas fazendas, por exemplo, 100 milhões de dólares e programar esse dinheiro para ser enviado a certos comerciantes de fertilizantes em um determinado momento, e que cada um só possa gastar no máximo 10 milhões de dólares por ano.

Em suma, uma CBDC poderia facilitar um estado centralizado mais eficiente. Isso dificilmente é uma coisa boa.

Outro item da agenda do governo e dos bancos centrais são as taxas de juros negativas. Os juros negativos ocorrem quando os depositantes não recebem juros sobre o dinheiro mantido em suas contas; em vez disso, eles pagam juros ao banco por reter seu dinheiro. Esse é uma fábrica de dinheiro para os bancos. Também incentiva as pessoas a gastar porque o dinheiro se desgasta se não for gasto, e os gastos do consumidor parecem sustentar a economia.

A crise bancária de 2015 na Grécia é um exemplo de como os juros negativos funcionam. Para evitar corridas bancárias, a Grécia impôs uma sobretaxa de um euro por 1.000 euros em saques em dinheiro. Salerno observa: “Não parece muito grande, mas o *princípio* em ação é extremamente grande porque o que eles estão fazendo é quebrar a taxa de câmbio entre uma unidade de depósitos bancários e uma unidade de moeda.” Salerno continua: “Para facilitar os cálculos […] digamos que a ‘sobretaxa’ grega é de dez dólares para cada 100 dólares sacados. Agora, em vez de poder converter um euro em sua conta corrente em um euro em dinheiro, sob demanda, você só poderá comprar um euro em dinheiro gastando 1,10 euros em suas contas bancárias. Isso é uma taxa negativa de 10% em algum sentido. […] Então, você realmente só receberia noventa centavos para cada dólar que você quisesse sacar e isso é muito significativo pois significa que será mais caro comprar um item com dinheiro do que com depósitos bancários.” Previsivelmente, as pessoas foram afastadas do dinheiro. Havia um incentivo para pagar contas domésticas a partir de suas contas bancárias, o que tornava todos os pagamentos rastreáveis.

O principal problema com um esquema de juros negativos para o governo e os bancos centrais é que as pessoas manterão seu dinheiro fora do sistema financeiro. Quantias grandes irão se manter além do alcance do governo. Se, entretanto, o dinheiro digital for totalmente adotado, então o governo pode insistir que as pessoas o usem em vez de dinheiro digital para pagamentos tais como impostos. Isso significa que a riqueza ficará presa no sistema financeiro.

A estratégia das corretoras centralizadas

> A raiz do problema com a moeda convencional é toda a confiança necessária para fazê-la funcionar [...] Temos de confiar a elas [terceiras partes] nossa privacidade, confiar que elas não permitam que ladrões de identidade [incluindo o governo] drenem nossas contas.
> – Satoshi Nakamoto

A única coisa a que as CBDCs não podem sobreviver é a competição de livre-mercado. É por isso que todo estado que busca uma CBDC fará um esforço conjunto para eliminar ou aleijar as alternativas de livre mercado. Um aspecto interessante dessa repressão é que existe uma forma de cripto não estatal que a maioria dos governos tolerará: moedas digitais emitidas por instituições financeiras licenciadas. Essas moedas não são um desafio para o sistema bancário central porque as instituições emissoras são regulamentadas para agir como se fossem bancos afiliados. Corretoras licenciadas tornam-se o lobby externo do sistema bancário central. O lobby imita o livre mercado de algumas maneiras, mas não tem nenhuma relação real com ele.

Uma definição padrão de uma corretora centralizada: “As corretoras de criptomoedas centralizadas são plataformas online usadas para comprar e vender criptomoedas. Eles são os meios mais comuns que os investidores usam para comprar e vender reservas em criptomoedas.” Uma corretora centralizada é um mercado para negociar ou converter ativos por meio de um único local ou serviço. No entanto, a definição não captura os problemas que as corretoras centralizadas apresentam ao modelo Satoshi.

Mas, primeiro, quais são os problemas que as corretoras centralizadas resolvem? Por que elas vieram a existir? Há uma demanda de mercado para especular, negociar moedas e realizar outras transações financeiras sofisticadas para as quais as estruturas peer-to-peer – corretoras descentralizadas – ainda não estão adequadamente equipadas. Há também uma demanda por conveniência e acesso a cripto que não requer conhecimento técnico ou esforço. Para alguns, as corretoras centralizadas também têm a familiaridade reconfortante dos bancos. Ou elas preenchem um nicho ou então elas não seriam populares. Atualmente, elas dominam grande parte do mundo das criptos, com a maioria dos usuários confiando às corretoras sua riqueza e privacidade.

O nicho ocupado pelas corretoras centralizadas vem da combinação das funções de um mercado de ações com a de um banco. De muitas

maneiras, elas são semelhantes à Bolsa de Valores de Nova York. Moedas podem ser negociadas, vendidas e sacadas por moeda fiduciária, por exemplo; o trading à margem, stop loss e empréstimos também estão disponíveis. De outras maneiras, as corretoras centralizadas se assemelham aos bancos tradicionais. Depois de comprar cripto de uma corretora, muitos clientes escolhem deixar suas moedas em uma conta em vez de transferi-las para suas carteiras privadas em seus próprios discos rígidos. As corretoras centralizadas tornam-se terceiras partes confiáveis; isso significa que elas representam um perigo terrível para a riqueza e o bem-estar dos titulares de contas. Considere um aspecto do risco. A maioria das corretoras centralizadas possuem as chaves privadas dos titulares das contas. Mas as chaves privadas *são* as criptos. As moedas não possuem presença física, apenas algorítmicas. Quando uma corretora controla as chaves, ela de fato é proprietária das moedas. O cliente não tem nada mais do que uma promessa de acesso a elas sob demanda, da mesma forma que os bancos prometem acesso a dinheiro físico mediante solicitação de um titular de conta.

Recentemente, os riscos associados às corretoras centralizadas aumentaram exponencialmente e por um motivo: as corretoras estão cada vez mais cumprindo ou fazendo parceria com o estado para fazer cumprir as leis e os requisitos de relatórios aos clientes. Um artigo da *Forbes* de fevereiro de 2018 anunciou o inevitável em relação à maior corretora centralizada do mundo.

> Finalmente está acontecendo: A movimentada movimentação de documentos na batalha entre o Internal Revenue Service (IRS) e a Coinbase, uma empresa que facilita transações de moedas digitais como Bitcoin e Ethereum, está avançando. A Coinbase anunciou que notificou os clientes afetados de que cumprirá uma ordem judicial em relação à liberação de dados específicos.

2018 foi o ano em que as agências fiscais americanas levaram a sério os lucros e reservas em criptomoedas. Governos de todo o mundo estão observando a Coinbase fornecer dados sobre seus clientes, o que quase certamente levará a auditorias e/ou processos judiciais de alto nível. Especificamente, a Coinbase está relatando todos os clientes com transações de $20.000 ou mais em um único ano entre 2013 e 2015.

Serão entregues identidades, nomes reais, datas de nascimento, endereços e todos os registros de transações. A riqueza de dados está disponível porque a Coinbase, como qualquer outra corretora licenciada, está em conformidade com as leis de Know Your Customer e Anti-Lavagem de Dinheiro que destroem a privacidade financeira.

A Coinbase se tornou extremamente agressiva na coleta de informações e na verificação de identidades. A corretora usa a tecnologia de reconhecimento facial, por exemplo, para comparar uma foto de rosto em tempo real de uma webcam ou smartphone com qualquer documento de identidade enviado pelo candidato. Espere que a intrusão agressiva se torne a norma para trocas centralizadas porque elas valorizam suas licenças e relacionamentos com o governo. Espere que elas atuem como braços de coleta de dados do estado. O perigo não é apenas o congelamento e confisco de contas, mas também os processos judiciais e a prisão dos titulares de contas. O IRS declara que "qualquer pessoa condenada por evasão fiscal está sujeita a uma pena de prisão de até cinco anos e uma multa de até $250.000. Qualquer pessoa condenada por apresentar uma declaração falsa está sujeita a uma pena de prisão de até três anos e multa de até $250.000."

Felizmente, a demanda do mercado para o mercado de ações e por funções bancárias pode ser satisfeita (ou em breve será satisfeita) sem sacrificar a privacidade e a segurança. Uma corretora descentralizada é um mercado que não depende de serviços de terceiros. As negociações são peer-to-peer; são transferências diretas entre pessoas que utilizam um processo automatizado para facilitar a troca. Elas são isentas da necessidade de confiança. Elas são transparentes, com o software e suas transações sendo de código aberto. Elas são Satoshi.

Uma corretora descentralizada permite que os indivíduos mantenham suas próprias chaves privadas, o que a torna um alvo menos atraente para hackers. Também requer uma quantidade mínima de dados pessoais ou financeiros para estabelecer uma conta e realizar comércio. Muitas vezes, apenas um endereço de e-mail é solicitado e pode ser gerado especificamente para registro, sem conexão com uma identidade real.

As corretoras descentralizadas empregam uma ampla variedade de estratégias para facilitar as transferências peer-to-peer. Alguns criam tokens proxy; outros empregam um depósito de múltiplas assinaturas. O banco peer-to-peer usa uma dinâmica do tipo leilão para facilitar em-

préstimos de um valor específico e a uma taxa acordada entre os membros. Os contratos inteligentes podem assumir as funções tradicionais dos bancos. A *Technology Review* explica:

Alternar entre dinheiro fiduciário e criptomoeda exigirá um ponto de troca tradicional no futuro próximo. Mas alguns tecnólogos dizem que é possível um modelo alternativo para negociar criptomoedas que daria às pessoas mais controle sobre sua riqueza. Suas metacorretoras podem ser descentralizadas, eles dizem, usando uma blockchain. A ideia depende especificamente dos chamados contratos inteligentes, código de software que pode ser armazenado em uma blockchain e configurado para controlar as transações programaticamente. Imagine, por exemplo, que você queira enviar a seu amigo alguma criptomoeda automaticamente em uma data e hora específicas. Você pode usar um contrato inteligente para fazer isso.

A questão aqui é *não* defender uma tática de descentralização específica. É oferecer uma noção das alternativas ricas e em evolução às corretoras centralizadas. Muitas pessoas ainda escolherão uma corretora centralizada porque as plataformas são fáceis de acessar e usar; eles são sancionados pelo governo e isso significa respeitabilidade para algumas pessoas; e oferecem as funções familiares e avançadas de um mercado de ações. As pessoas têm todo o direito de fazer essa escolha com seu próprio dinheiro, é claro. Mas para aqueles que valorizam a privacidade, é uma alternativa inaceitável. (Mais sobre corretoras descentralizadas posteriormente).

Uma analogia ilustra a diferença gritante em como a privacidade e os direitos se comportam em um sistema centralizado e descentralizado: mídia social.

"'Quer enlouquecer?' Aqui estão todos os dados pessoais que o Facebook/Google coleta". Esta é uma manchete de março de 2018 em *Zero Hedge*. Os tipos de dados coletados são extensivos demais para enumerar. Um exemplo: Os usuários de celulares Android que baixaram aplicativos específicos do Facebook tiveram dados sobre suas chamadas pessoais registradas pelo Facebook por anos.

Uma causa relativamente não discutida da hemorragia de privacidade das mídias sociais e sua abreviação da liberdade de expressão é a centralização de informações e discussões que acompanham as empresas gigantes, como Facebook e Google. Grandes corporações formam alianças de conveniência e lucro recíproco com o governo. Um artigo intrigante no *The Federalist* pergunta: "As mídias sociais foram um

erro?” O autor, Robert Tracinski, remonta aos anos 2000 – a era de ouro dos blogs, quando todos, até suas avós, se expressaram através de blogs.

Tracinski escreve: “Parecia uma liberação. A era dos blogs ofereceu a promessa de uma mídia descentralizada. Qualquer um poderia publicar e comentar as notícias e encontrar uma audiência. [...] Estávamos ignorando os antigos guardiões da mídia. E tivemos o controle sobre eles! Nós postamos em nossos próprios sites. Tivemos boas discussões sobre nossos campos de comentário, os quais nós moderamos.” Era um turbilhão de liberdade de expressão, mas também era um bastião de privacidade porque os indivíduos mantinham o controle. O controle individual de dados e expressão é liberdade.

Então as mídias sociais chegaram como um rolo compressor, e os blogs familiares migraram seus diários e informações para o Facebook, Google, Twitter e outras terceiras partes confiáveis. Assim como as corretoras centralizadas, os gigantes da mídia social eram relativamente fáceis de acessar e usar; eles ofereciam software e funções sofisticadas que os blogueiros individuais não tinham conhecimento técnico ou dinheiro para implementar; as mídias sociais deslizaram perfeitamente para os telefones celulares por meio de aplicativos que pareciam abrir o mundo. Na realidade, eles fecharam a libertação pessoal.

Tracinski observa o resultado.

> Alguns dos melhores e mais interessantes blogs tornaram-se publicações on-line completas, mas muitos dos pequenos, peculiares e amadores blog de uma só pessoa se mudaram para as mídias sociais. Isso se mostrou como um grande erro, porque a era da mídia social *re-centralizou* a mídia. Em vez de um milhão de blogs – o que Glenn Reynolds, famoso pelo Instapundit, chamou de “Exército de Davids” – agora temos uma economia de mídia social controlada principalmente por três grandes empresas: Twitter, Facebook e Google.

O preço de centralizar a escrita pessoal tornou-se aparente. A política esquerdista dos gigantes da mídia social significa que eles purgam (suspenderam contas) ou puniram (contas limitadas) aqueles que têm opiniões “erradas”. Isso é semelhante a bancos e outras instituições financeiras que se recusam a lidar com pornografia, maconha ou indús-

trias de armas devido à pressão política do governo. Os "antigos guardiões da mídia" foram substituídos pelos puritanos igualmente intrusivos do Vale do Silício. Embora ambos possam ser preferíveis à intervenção direta do governo, seus quase monopólios são reforçados por privilégios fiscais, por regulamentação favorável e por financiamento de impostos diretos. Em suma, eles podem não ser do governo, mas certamente são comparsas do estado e devem sua lealdade a ele. Como resultado, os indivíduos perderam o controle de seu próprio trabalho e dados. Talvez seja mais correto dizer que eles o abandonaram.

Em nenhum lugar o preço da centralização da expressão pessoal é mais gritante do que com os dados pessoais. Em retorno pela conveniência, tudo o que as mídias sociais pediam era conhecer e comercializar cada detalhe da vida dos clientes. O papel da centralização nesse estupro da privacidade foi fundamental para sua eficácia.

A Privacidade é a linha de frente da defesa da liberdade individual. A descentralização é a condição social sob a qual a privacidade prospera. Ninguém pode ou deve dizer aos indivíduos qual estratégia usar. Mas, se você valoriza privacidade e segurança, mantenha a privacidade e descentralize.

SEÇÃO DOIS

O Imperativo da Privacidade

Quando a Privacidade é Criminalizada, Apenas os Criminosos têm Privacidade

> "Eu cresci entendendo que no mundo em que eu vivia as pessoas desfrutavam de uma espécie de liberdade para se comunicarem umas com as outras em privacidade, sem serem monitoradas, medidas, analisadas ou julgadas por essas figuras e sistemas sombrios que vivem mencionando o tempo todo na mídia."
> – Edward Snowden

Quero a seguinte mensagem escrita em minha lápide: "Eu vivi. Eu morri. Agora cuide da sua maldita vida." O que eu teria a esconder? Tudo! Que é o mesmo que dizer: qualquer informação que eu seja obrigada a revelar são dados que eu me recuso a divulgar.

No entanto, uma questão fundamental paira sobre essa retórica fervorosa e rebelde:

O que é Privacidade?

Uma resposta famosa vem de um artigo dos advogados americanos Samuel Warren e Louis Brandeis, que apareceu em uma edição de 1890 da *Harvard Law Review*. É uma das peças mais influentes na história da teoria jurídica ocidental. "The Right to Privacy" foi chamado de primeiro apelo proeminente para a privacidade como um conceito a ser consolidado na lei.

O artigo começa da seguinte maneira:

> "QUE o indivíduo deve ter plena proteção pessoal e patrimonial é um princípio tão antigo quanto o direito comum; mas foi considerado necessário, de tempos em tempos, definir novamente a natureza exata e a extensão de tal proteção."

Em outros lugares, a privacidade é definida como o direito de ser deixado em paz.

O artigo defende a privacidade como um direito humano "fundamental" ou básico sobre o qual repousam todos os outros direitos. "O direito de propriedade em seu sentido mais amplo, incluindo todos os direitos e privilégios e, portanto, abrangendo o direito a uma personalidade inviolável, justifica sozinho aquela ampla base sobre a qual pode repousar a proteção que o indivíduo exige". A privacidade é um pré-requisito para todos os outros direitos: liberdade de expressão, sexualidade, liberdade de consciência e segurança financeira dependem disso, porque nenhum direito pode ser exercido na presença de storm troopers batendo à porta. E por isso o direito de trancar essa porta é essencial.

Curiosamente, o artigo de Brandeis-Warren foi uma resposta a desenvolvimentos tecnológicos que ameaçavam a privacidade pessoal. Um dos desenvolvimentos foi a câmera portátil, com a qual jornalistas fotografavam pessoas importantes em locais que antes eram privados, como restaurantes, casamentos e funerais. Hoje, o foco da proteção da privacidade mudou dos jornalistas para o estado, para o qual "privacidade" é sinônimo de "sigilo". A privacidade não é mais um direito, mas uma provável causa de suspeita. A mudança na definição reflete o quão poderoso o estado se tornou desde a década de 1890 – e o quão enfraquecido se tornou o indivíduo.

Embora a privacidade tenha sido um tema tanto no direito consuetudinário quanto nas sociedades ocidentais, seu status legal tem sido vago. De fato, antes do "Direito à Privacidade", a proteção legal da privacidade era fragmentada em questões específicas. Leis contra invasão existiam, por exemplo, mas a codificação do conceito amplo de privacidade não existia.

Afinal, o que significa o "direito de ser deixado em paz"? Grande parte deste capítulo explora uma resposta.

Todo mundo sabe que a bolsa de uma mulher não deve ser roubada, nem sua janela espiada e tão pouco sua casa assaltada. Esses são obviamente e intuitivamente casos de violações de privacidade, mas não são o tipo de violação que os usuários de criptomoedas provavelmente enfrentarão. Os usuários de criptos lidarão com suas informações pessoais sendo extraídas e monitoradas – muitas vezes secretamente – para serem usadas contra eles de alguma maneira. Com o estado, o objetivo da extração de dados e do monitoramento é o controle social, a tributação, o confisco e a prisão. Com criminosos, o objetivo é o roubo, a chantagem e a extorsão.

Espiar pela janela do quarto pode ser uma violação óbvia de privacidade, mas e os bisbilhoteiros que acessam informações públicas, como as incorporadas à blockchain? O registro financeiro aberto da blockchain permite que partes indesejadas monitorem transações financeiras que os usuários tornam públicas voluntariamente. Se um bisbilhoteiro analisa o padrão de transferências e desmascara a identidade de um usuário, então a privacidade foi violada? A blockchain é uma rede pública, onde as pessoas trocam voluntariamente de uma maneira que sabem ser transparente e registrada. Espionagem é semelhante a ouvir pessoas que estão falando audivelmente em público. Mas será que ouvir é um ato culposo, especialmente quando feito por agentes do estado ou outros maus agentes? De fato, o estado e outros criminosos usam a informação de maneira maléfica, mas essa questão é irrelevante para definir se o ato de simplesmente ouvir é errado em si.

Avaliar essa questão significa colocar a privacidade no contexto de outros direitos humanos.

O contexto dos direitos humanos à privacidade

Murray Rothbard afirma que todos os direitos humanos são direitos de propriedade. Ou seja, todos os direitos se resumem à questão de quem controla adequadamente o uso e o descarte de uma coisa, seja a coisa uma ferramenta, uma ideia ou um corpo humano. É sempre possível usar a força para usurpar o controle de qualquer coisa, é claro, mas a questão de quem é o proprietário *adequado* permanece.

Rothbard responde: O proprietário é o indivíduo que detém o título válido da coisa. A verdadeira propriedade não é uma questão de *puro* controle, que pode ser adquirido através da força bruta, mas de controle legítimo, que vem da aquisição pacífica do título. Não pode haver título mais óbvio ou válido do que aquele que os indivíduos têm sobre seus próprios corpos. De fato, tentar negar esse título se reduz à obscenidade ou ao absurdo. Existem apenas três posições possíveis sobre quem possui o corpo de uma pessoa: a própria pessoa (liberdade), outra pessoa (escravidão), ou é bagagem não reclamada. Aqueles que valorizam a liberdade e os direitos humanos defendem a autopropriedade.

Novamente, a definição clássica de autopropriedade: todo ser humano tem jurisdição moral e lógica sobre seu próprio corpo e o uso

pacífico dele, incluindo os produtos de seu trabalho. Nenhum direito é mais fundamental do que a autopropriedade, porque ela é a própria fonte de todos os outros direitos. A liberdade de consciência e de expressão só existe porque os indivíduos têm a capacidade de pensar e falar, e ambos são aspectos do corpo humano. O direito de autodefesa existe apenas porque as pessoas são donas de seus corpos e têm o direito de proteger sua propriedade. O outro lado dos direitos é o dever. Assim como todos os outros seres humanos são moral e logicamente proibidos de iniciar a força contra você, você tem o dever de desistir de iniciar a força contra eles.

Se existe um direito à privacidade, então ele deve estar enraizado na autopropriedade. Deve ser o que se chama de direito natural. E, se a privacidade é um direito, outras pessoas têm o dever de desistir de violá-la.

A questão não é trivial. A propriedade de si mesmo e a privacidade estão ambas sob o constante ataque do maior bisbilhoteiro da história: o estado. O estado, com extremo preconceito, pretende usar os dados que coleta contra as pessoas. Em seu livro, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, o cientista político James C. Scott comenta o papel que apenas uma forma de coleta de dados desempenhou na ascensão do estado moderno: o censo. “Se imaginarmos um estado que não tem meios confiáveis de enumerar e localizar sua população, medir sua riqueza e mapear suas terras, recursos e assentamentos, estamos imaginando um estado cujas intervenções nessa sociedade são necessariamente brutas.” O estado atual é sofisticado e complexo.

Informação é poder, tanto para o indivíduo quanto para o estado. Uma razão pela qual o estado consegue adquirir dados é que a privacidade é um conceito mal definido que as pessoas não entendem como parte do contexto mais amplo dos direitos. Outra razão é que a informação é efêmera e parece menos propensa à posse do que uma mesa ou um carro.

A avaliação de se a privacidade de dados é um direito natural depende de duas questões. Como um prelúdio para considerá-las, pondere se você tem o direito de propriedade sobre seus pensamentos e sua expressão, incluindo a expressão de informações pessoais. Essa ampla indagação é fundamental para a questão da propriedade intelectual, que é a afirmação de que as ideias e suas expressões podem ser possuídas. As

pessoas chegam a conclusões dramaticamente diferentes, e a propriedade intelectual é frequentemente reivindicada como um direito natural. A mesma questão confronta a privacidade, que também aborda a propriedade das informações pessoais e a expressão delas.

Pergunta # 1: *Quem é o dono do que está na sua mente?*

A maioria das pessoas declararia em voz alta: "ninguém é dono do que está em minha mente!". Seus pensamentos são seus pela mesma razão que seus dedos e olhos; eles são parte de seu corpo, e seu corpo é quem você é. É você. Ninguém mais tem o que clamar ao reivindicar jurisdição sobre seu corpo. Mas e se o pensamento em sua mente for uma fórmula química originada por um colega de trabalho e escrita em um quadro-negro durante uma palestra que você assistiu? A fórmula agora faz parte da sua mente, assim como da dele e, se ele pode reivindicar o direito de usá-la porque faz parte do corpo dele, você não deveria poder fazer a mesma reivindicação?

Nesse ponto, o argumento do colega de trabalho geralmente muda de terreno. Ele *originou* a ideia, diz ele; a fórmula é um produto de seu trabalho, e possuir os produtos de seu trabalho é uma extensão da propriedade de si mesmo. Não importa se a ideia está em *sua* mente agora; é ideia *dele*. Ele a encontrou primeiro.

Deixando de lado o fato de que o colega de trabalho provavelmente utilizou as ideias e o trabalho de centenas de pessoas antes dele – ou seja, a fórmula também é produto do trabalho deles – vamos supor que ele adicionou um refinamento totalmente original. O que é que tem? No instante em que você vislumbrou a fórmula, o conceito mudou. A fórmula foi integrada a todos os outros conceitos que você tem sobre química, tecnologia e vida em geral. A fórmula em sua mente é ligeiramente ou consideravelmente diferente daquela no quadro-negro ou na mente de seu colega de trabalho. Como então ele pode reivindicar direitos de propriedade em uma ideia baseada no trabalho anterior de outras pessoas enquanto nega seus direitos de propriedade em uma ideia baseada em seu trabalho anterior?

A linha de chegada do cenário: ninguém tem direito ao que está em sua mente. O que é chamado de privacidade nesta circunstância se reduz à autopropriedade. Você é dono daquilo que está sob sua pele, incluindo as suas ideias. O libertário do século XIX James Walker afirma: "Meus pensamentos são minha propriedade, assim como o ar em meus pulmões é minha propriedade […]" Quando você expira, no

entanto, você perde todo o direito de propriedade do ar expelido. O mesmo vale para ideias ou informações que são lançadas na esfera pública; você perde todas as reivindicações de privacidade, exceto e a menos que haja um acordo prévio de confidencialidade em vigor. Nessas circunstâncias, sua reivindicação de privacidade ou propriedade de informações não é uma questão de direitos naturais, mas de direitos contratuais.

O paralelo com as informações financeiras: os usuários de cripto perdem qualquer expectativa razoável de privacidade ou propriedade das informações quando elas entram na blockchain ou em outra esfera pública. Um bisbilhoteiro que acessa os dados nada mais faz do que ver aquilo que é de conhecimento e acesso público. O bisbilhoteiro pode usar o conhecimento de forma que prejudique um usuário, mas o uso da informação é uma questão diferente de como ela foi obtida.

Pergunta #2: *Como os dados foram obtidos?*

A resposta a esta pergunta é distinguir entre a espionagem legítima e o ato criminoso. Bisbilhoteiros legítimos não fazem mais que acessar informações divulgadas publicamente ou livremente e, ainda que sejam inconvenientes, de forma alguma violam direitos. Por outro lado, bisbilhoteiros criminosos violam direitos de propriedade privada para acessar dados. Tocar em um telefone ou computador é como invadir a casa de uma pessoa para vasculhar um arquivo ou uma mesa. Um recenseador que ameaça uma pessoa que não responde com multas ou prisão está usando meios criminosos para acessar informações. O teste decisivo para distinguir entre espionagem legítima e espionagem crime é se a aquisição de dados envolve uma violação de direitos.

Rothbard argumenta que "não existe direito à privacidade, exceto o direito de proteger a propriedade de uma invasão". Em outras palavras, não há direito natural à privacidade per se. A informação é privada em virtude de estar protegida por outros direitos. Uma pessoa tem o direito de ocultar informações, por exemplo, porque o direito à liberdade de expressão inclui o direito de permanecer em silêncio, e quebrar um determinado silêncio requer ameaças ou violência. Da mesma forma, uma pessoa tem o direito de fechar a porta atrás de si, e as informações nos papéis em sua mesa são protegidas de intrusos por seu direito de propriedade sobre a casa. A privacidade da informação é protegida pelo muro de direitos que a cerca, mas isso não faz da privacidade um direito em si.

Por outro lado, se uma pessoa grita informações pessoais em praça pública ou se joga seus papéis pela janela ao vento, seus dados não estão mais protegidos por seus direitos de propriedade. A pessoa os colocou na esfera pública e abandonou a reivindicação de controle exclusivo.

A abordagem Satoshi da privacidade tem um pé em ambos os mundos – abandono público de informações junto com privacidade protegida por direitos naturais. Uma blockchain transparente funciona com usuários anônimos ou pseudônimos que empregam chaves públicas e privadas. Os dados sobre as transações foram jogados ao vento, mas as identidades são protegidas por outros direitos. Em outras palavras, desmascarar a identidade de alguém ou sua chave privada requer uma violação dos direitos de propriedade que os cercam e protegem – o direito da pessoa ao seu computador, por exemplo. A propriedade consiste no direito exclusivo de controlar e usar uma coisa; se o estado acessar um computador sem considerar o consentimento do proprietário real, então o estado está usurpando a propriedade do computador e violando descaradamente os direitos do proprietário real.

Uma mudança dramática no paradigma da privacidade

A abordagem Satoshi pode confundir algumas pessoas. Enquanto elas se apegarem ao velho paradigma de privacidade – isto é, privacidade é igual a ocultação – a transparência da blockchain continuará a soar como uma sentença de morte. Mas o novo paradigma da privacidade é a transparência das informações e a proteção da identidade. O foco mudou de informações sobre atividades para informações sobre nomes verdadeiros.

A transparência das transações serve a um propósito vital. Por uma questão de honestidade e eficiência, a blockchain publica todas as suas atividades. A proteção dos Nomes Verdadeiros também serve a um propósito vital. Por uma questão de liberdade pessoal, os participantes mascaram suas identidades à vontade e com facilidade. A blockchain exige a verificação de identidade tanto quanto uma mercearia exige o registro dos nomes daqueles que compram leite nela. Que todos vejam, que todos verifiquem a veracidade da transação. Que ninguém exija informações pessoais sobre quem é o porquê da troca. Tanto a honestidade

quanto a privacidade são preservadas, mas o vínculo entre uma transação e um Nome Verdadeiro é quebrado. O restabelecimento forçado desse vínculo ameaça a riqueza e a liberdade dos usuários.

No passado, o foco do estado era a divulgação ou vigilância forçada de informações sobre atividades, porque o estado havia encurralado a “indústria da identidade”. Desde o nascimento, as pessoas são registradas, certificadas, gravadas e processadas de acordo com os números e outros identificadores emitidos pelo estado. David Friedman observa em seu ensaio “The Case for Privacy”, “É difícil passar pelo mundo sem deixar rastros. Em algum lugar há um registro de todos os carros que comprei, todos os formulários de impostos que paguei, dois casamentos, um divórcio, o nascimento de três filhos, milhares de postagens em fóruns on-line sobre uma ampla variedade de assuntos, quatro livros publicados, registros médicos e muito mais.”

A identidade e o Nome Verdadeiro dos indivíduos são muito mais conhecidos do que suas interações, muitas das quais podem ocorrer em segredo e silêncio. O modelo Satoshi inverte essa situação. Ele torna todas as interações públicas com todas as identidades permanecendo privadas a critério dos indivíduos. O estado não controla mais a identidade e, sem esse controle, o acesso a todas as outras informações têm pouco valor. E o estado sabe muito bem disso.

A era digital mudou o Zeitgeist cultural, político e psicológico da privacidade. “Cuide da sua maldita vida!” já foi uma atitude respeitada, mas o estado lentamente corrompeu a ideia de que pessoas inocentes precisam de privacidade. Eis o novo Zeitgeist: apenas aqueles que têm algo a esconder se recusam a responder a perguntas ou a serem observados. “Só os criminosos temem a vigilância do estado” é uma resposta comum para quem defende a privacidade hoje. Mas toda pessoa pacífica é agora um criminoso com algo a esconder. Por quê? Porque todos ultrapassaram o limite de velocidade, usaram drogas ilegais, contrabandearam bebidas baratas ou cigarros através da fronteira, fizeram acréscimos “não autorizados” a um imóvel, enganaram um agente do estado, sonegaram sua renda ou violaram uma das dezenas de milhares de leis estatais que criminalizam o comportamento inofensivo de maneira onipresente. A maioria das pessoas não está ciente de quantas leis eles quebram no decorrer de uma vida cotidiana pacífica.

Quando a Privacidade é Criminalizada, Apenas os Criminosos têm Privacidade

Em seu livro *Three Felonies A Day: How the Feds Target the Innocent*, o advogado Harvey Silverglate detalha como o americano médio acorda e segue sua rotina diária, sem saber que provavelmente cometerá vários crimes federais ao fazê-lo. O número de crimes federais aumentou exponencialmente nas últimas décadas e os promotores agora podem escolher entre uma infinidade de crimes vagamente definidos para acusar indivíduos pacíficos de todas as origens, profissões e status. Uma combinação de leis amplas e mal definidas, a guerra às drogas e promotores de carreira que são imunes às consequências transformaram a justiça em uma burocracia livre de consciência, onde parece não haver espaço para a inocência ou culpa. Silverglate observa um procedimento padrão para os burocratas da justiça:

> Os promotores são capazes de estruturar acordos de delação premiada, de maneira que torna quase impossível para pessoas normais, racionais e calculistas se arriscarem a ir a julgamento. A pressão sobre réus inocentes para se declararem culpados e "cooperar" testemunhando contra outros em troca de uma sentença reduzida é enorme – tão grande que essas testemunhas que cooperam muitas vezes deixam de dizer a verdade, dizendo, em vez disso, o que os promotores querem ouvir.

O livro de Silverglate evoca uma assustadora citação infame da era soviética, dita pelo desprezado Beria, chefe da polícia secreta de Stalin. "Mostre-me o homem, e eu encontrarei o crime para você." Quando alguém lhe perguntar: "O que você tem a esconder?", você deve responder: "De Beria e sua laia, tudo, especialmente minha identidade (o homem)."

Ou, como Ayn Rand explicou certa vez: "O único poder que qualquer estado tem é o poder de reprimir os criminosos. Bem, quando não há criminosos suficientes, eles os criam. Declara-se que tantas coisas são crime que se torna impossível para os homens viverem sem infringir as leis."

Os usuários de cripto que exigem privacidade são especialmente vulneráveis a suposições culturais e políticas que favorecem fortemente o controle estatal em vez da liberdade individual.

As fortes suposições contra a privacidade incluem:

- A presunção da inocência pertence ao estado, e não aos indivíduos.
- Um duplo padrão de moralidade é aplicado ao estado e aos indivíduos.
- A privacidade é equiparada à ocultação.

A Presunção da Inocência. O termo legal "presunção da inocência" às vezes é expresso pela frase latina "*ei incumbit probatio qui dicit, non qui negat*", que significa que o ônus da prova é do acusador, e não do acusado. O acusado é presumido inocente até que se prove o contrário. A doutrina jurídica baseia-se na crença de que a maioria das pessoas não são criminosas, de modo que a criminalidade não pode ser presumida; ela deve ser demonstrada. A doutrina também reconhece um princípio fundamental da lógica: por ser impossível provar uma negativa, o ônus da prova recai sobre a pessoa que faz uma afirmação positiva. Alguém pode alegar que você é um ladrão. E mesmo evidências massivas de sua honestidade não dissiparão a acusação, porque você pode estar mentindo sobre um delito passado ou ocultando evidências. É por isso que o acusador é solicitado a especificar o que você roubou e a fornecer provas do crime.

A presunção da inocência é a pedra angular do devido processo legal e um muro de proteção contra processos arbitrários por parte do estado. É uma característica definidora de uma sociedade livre em oposição a uma totalitária. O renomado advogado britânico Sir John Clifford Mortimer – mais conhecido como o criador do amado advogado de defesa fictício Horace Rumpole – estava longe de ser o único a ver a presunção da inocência como "o fio de ouro" que une a justiça.

Mas o fio de ouro foi rompido.

Em nome da segurança, o público perdeu a presunção da inocência mesmo na ausência de acusações. Agentes de fronteira e aeroporto tiram impressões digitais, revistam, interrogam e ladram "Seus documentos!" para hordas enfileiradas. Indivíduos que não cumprem são automaticamente retirados da linha e processados como criminosos. Os policiais exigem identidade e prendem aqueles que se recusam, independentemente de a prisão ser legal ou não. Afinal, supõe-se que os agentes estatais protejam a segurança e imponham a paz. Isso significa que aqueles que resistem são contra a segurança e a paz. Poucas pessoas

perguntam de onde a imposição da lei obtém o direito de exigir obediência de pessoas que não estão causando danos. A presunção de inocência foi transferida dos indivíduos para os agentes estatais, o que inverte a intenção original do conceito legal de proteger os indivíduos *do* estado.

O princípio lógico de ser incapaz de provar uma negativa foi substituído pela falácia conhecida como “o argumento ou apelo à ignorância”. Aqui, “ignorância” refere-se à falta de evidência contrária – uma situação considerada suficiente para provar a verdade de uma afirmação. Em suma, uma acusação é verdadeira porque não se prova que seja falsa. A criminalidade de um indivíduo torna-se um dado porque não é refutada. Por que mais, pergunta o estado, ele se recusaria a cooperar com as autoridades?

É difícil exagerar a importância da mudança na presunção da inocência do indivíduo para os agentes estatais. Assim como a presunção da inocência é o fio de ouro da justiça, a presunção da culpa para os indivíduos é sua morte. Isso oblitera o devido processo e leva a sociedade diretamente para o totalitarismo. Esse é o significado político e a consequência da “inocente” pergunta: “O que você tem a esconder?”. A identidade emitida pelo estado é crucial para o processo. Depois que seu Nome Verdadeiro é conhecido, então todos os outros controles sociais se tornam possíveis.

Um duplo padrão de moralidade. Existem dois pesos e duas medidas em ação na sociedade – um para os indivíduos e outro para o estado. O que é imoral para um indivíduo, tornou-se moral para o estado. Se você pegar dinheiro de um vizinho sob a mira de uma arma, é um ato de roubo pelo qual você é preso com justiça. Se um agente do estado faz o mesmo, é um ato de tributação, pelo qual o malfeitor paga sua “justa parte” dos ganhos e pelo qual o agente recebe um salário e uma pensão. A moralidade moderna é agora definida por quem está realizando o ato, não pelo ato em si. O sigilo impenetrável do estado é prudente, enquanto a privacidade dos indivíduos é criminosa.

Nenhuma voz foi mais clara contra um duplo padrão de moralidade do que a do editor libertário Raymond Cyrus Hoiles, que criou a rede midiática Freedom Communications. Hoiles acreditava que o duplo padrão era mais destrutivo para a sociedade do que qualquer outro conceito, e seus ataques ferozes contra ele explodiam com frequência em seus jornais.

Em um editorial intitulado “O erro mais prejudicial que a maioria das pessoas honestas cometem” (17 de dezembro de 1956), publicado no *Santa Ana Register*, Hoiles explica o erro: “É a crença de que um grupo ou um estado seja capaz de fazer coisas que seriam prejudiciais e perversas se feitas por um indivíduo e produzir resultados que não sejam prejudiciais, injustos e perversos. É a crença de que um número de pessoas fazendo algo que é errado para um indivíduo pode resultar em algo correto e justo.” Hoiles mais frequentemente criticou o erro com referência à tributação. Novamente, se era errado um vizinho roubar seus bens, então era igualmente errado para um grupo de vizinhos ou seu representante designado (estado) realizar o mesmo ato.

A crítica de um duplo padrão não começou com Hoiles, é claro. Um panfleto de 1657 atribuído ao rebelde Coronel Titan argumenta: “O que pode ser mais absurdo na natureza e contrário a todo bom senso do que matar e chamar de Ladrão aquele que vem sozinho […] e obedecer e chamar de Lorde Protetor aquele que vem com regimentos e tropas? Se aquele que rouba e comanda dois ou três navios é chamado de pirata, por que aquele que rouba e comanda cinquenta é chamado de almirante?”. É esse o absurdo que o estado impõe quando faz algo que não seria tolerado caso fosse feito por um único indivíduo.

Mais uma vez, ninguém pergunta onde o estado adquire esses chamados direitos abrangentes. Como os únicos direitos que existem são os individuais, contra os quais ninguém pode legitimamente agredir, se o estado deseja reivindicar a propriedade legítima das informações privadas de terceiros deve apresentar prova de divulgação voluntária, transferência ou compartilhamento de título. Caso contrário, os chamados direitos nada mais são do que a afirmação da pura violência.

O que se aplica à tributação se aplica não menos à violação da privacidade. Se é errado um vizinho revistar seu corpo e o de seu filho sem consentimento, então é errado um agente do estado fazer isso em um aeroporto. Se é errado um vizinho grampear seu telefone, registrar suas transações financeiras e espiar pelas janelas, então é errado o estado fazê-lo. Os indivíduos de um grupo não renunciam à responsabilidade pessoal porque os atos são sempre cometidos por um indivíduo e são sempre uma questão de responsabilidade pessoal. O estupro coletivo não é menos que o estupro individual e os estupradores não são menos particularmente responsáveis porque foram o segundo ou o terceiro na fila.

No entanto, as pessoas aceitam um duplo padrão de moralidade, que isenta os agentes estatais de responsabilidades morais e legais. Se os agentes do estado, do presidente aos funcionários dos correios, estivessem sujeitos aos mesmos padrões de decência e responsabilidade legal que os indivíduos, o atual estado desmoronaria.

A privacidade é equiparada à ocultação. Redefinir "privacidade" como "ter algo vergonhoso a esconder" é um truque de mágica. Em seu excelente ensaio "I've Got Nothing to Hide' and Other Misunderstandings of Privacy", o professor Daniel J. Solove explica a mágica por trás da metamorfose da privacidade em ocultação: "O argumento de que não existe problema de privacidade se uma pessoa não tem nada a esconder é frequentemente feito. […] Quando o governo se envolve em vigilância, muitas pessoas acreditam que não há ameaça à privacidade, a menos que o governo descubra atividades ilegais, caso em que uma pessoa não tem justificativa legítima para alegar que isso deve permanecer privado". Curiosamente, as pessoas que usam o argumento de não ter "nada a esconder" também penduram cortinas nas janelas e as fecham ao se despir. Eles não dão suas carteiras ou bolsas para estranhos vasculharem. Eles fecham a porta antes de fazer sexo e se opõem que suas fotos nuas sejam postadas online. O que eles estão escondendo? Como Solove comenta: a privacidade "não é sobre nada a esconder, é sobre as coisas que não são da conta de ninguém."

O ataque à privacidade individual é tóxico para a sociedade como um todo.

Considere a liberdade de expressão. Lembro-me de estar em um restaurante quando um parente fez um discurso pós 11 de setembro sobre como a atmosfera nos EUA estava começando a parecer a da Cuba da qual ele havia fugido. Sua esposa tentou silenciá-lo, declarando em um sussurro inflexível: "Você não pode dizer essas coisas em público". Ela estava nervosa enquanto olhava ao redor para ver quem poderia ter ouvido. A vigilância e os informantes tornam as pessoas relutantes em expressar opiniões que podem ser usadas contra elas de maneira legal ou política. Propriedades podem ser apreendidas, famílias destruídas e pessoas presas. Por que alguém falaria o que pensa se como resultado seus filhos podem perder o pai deles?

Até recentemente, muitas incursões contra a privacidade não ocorriam apenas por serem difíceis de executar. Então a tecnologia chegou. A vigilância agora é muito mais eficiente, e requer menos esforço.

Mesmo burocracias notoriamente incompetentes são capazes de vigiar como nunca. Muitas pessoas estão com medo ou complacentes em relação à vigilância. Alguns simplesmente não acreditam mais na possibilidade de privacidade. O estado se beneficia imensamente da Grande Mentira de que a privacidade agora é impossível devido à onipotência e onisciência do estado. Isso é besteira. Em primeiro lugar, a tecnologia quase sempre empodera o indivíduo tanto ou mais do que o estado. Em segundo lugar, há um mundo de diferença entre o mais difícil e o impossível. A privacidade pode ser mais difícil do que antes ou, talvez, seus requisitos tenham apenas mudado e sejam necessárias proteções diferentes do que as de antes. Talvez a privacidade exija mais inovação e trabalho.

O valor da privacidade para a sociedade

Uma sociedade saudável requer privacidade. Quando um estado monitora a comunicação geral, as pessoas não interagem livremente. Isto é especialmente verdadeiro para dissidentes, os pacificamente aberrantes, escritores, delatores, usuários de drogas, críticos do estado, céticos, advogados de defesa, artistas … Quem é diferente no estilo de vida ou na opinião sente o calafrio de ser observado por autoridades que acenam com armas e celas de prisão. A sombria sociedade cinzenta da União Soviética e de outros estados comunistas fornecem uma lição de moral sobre como o medo esmaga a criatividade e a discussão. A vigilância despoja a sociedade de cor e vibração porque drena a vida dos indivíduos, e os indivíduos *são*, coletivamente, a sociedade.

Também impede que as pessoas se levantem contra a injustiça. A defesa da privacidade é uma defesa dos direitos humanos. Ainda assim, a privacidade financeira pode não ser a questão com a qual entrar na discussão desse vínculo, porque o dinheiro desperta cinismo imediato. Mas o vínculo deve ser estabelecido.

Considere a liberdade de religião e o devido processo legal. Uma insurreição do século XVI definiu a evolução desses dois, bem como sua conexão com a privacidade. A revolta girava em torno do direito de uma pessoa manter suas crenças religiosas privadas para que não pudessem ser usadas contra ela em um tribunal. Uma versão atual desse direito é chamada de “clamar a quinta” – invocando o devido processo

legal contra a autoincriminação. É chamado de "clamar a quinta" porque a Quinta Emenda da Declaração de Direitos dos EUA estabelece: "Nenhuma pessoa será obrigada em qualquer caso criminal a ser testemunha contra si mesma". Embora este pilar do devido processo seja frequentemente retratado como um recurso para o culpado, o grande beneficiário é o homem inocente na rua, que é protegido contra o exercício do poder arbitrário, quer ele perceba ou não.

A insurreição do século XVI: Henrique VIII negou a autoridade papal e estabeleceu a Igreja da Inglaterra, que reivindicou nova autoridade sobre as almas das pessoas. Os protestantes, chamados dissidentes, eram frequentemente julgados por heresia com tortura, geralmente acompanhando o julgamento. No final da década de 1530, o protestante John Lambert foi queimado vivo por heresia. Durante seu julgamento, Lambert se tornou o primeiro inglês conhecido a proclamar que era ilegal sob Deus e a lei comum obrigar um homem a se acusar. Ele apelou para a privacidade da consciência.

Em 1563, o dissidente John Foxe publicou o imensamente influente *Book of Martyrs*, um livro de história e martirológio protestante, que foi chamado de "cartilha libertária" sobre direitos processuais. Ele defende o direito de permanecer em silêncio para manter as informações pessoais privadas. Notoriamente, o leveller e libertário John Lilburne empregou os procedimentos de Foxe em 1637, quando foi levado ao Tribunal da "Star Chamber" (Câmara Estrela) por distribuir livros puritanos (o termo "Star Chamber" tornou-se sinônimo de tribunais elitistas e abusivos que se reúnem em segredo). Recusando-se a fazer o juramento costumeiro, Lilburne negou-se a responder perguntas que testemunhassem contra si mesmo. Ele foi multado, chicoteado, humilhado e condenado à prisão até que ele obedecesse. Enquanto estava lá, ele escreveu um relato de seu tratamento brutal, intitulado *The Work of the Beast*. Alguns anos depois, a tão odiada Star Chamber foi abolida e o direito de permanecer em silêncio – o direito à privacidade – foi estabelecido.

O direito contra a autoincriminação – o direito à privacidade das informações pessoais – está no cerne do devido processo legal. Está historicamente ancorado na busca pela liberdade religiosa, mas não se aplica menos a outras liberdades, inclusive às econômicas. A demanda por privacidade não apenas protegeu os indivíduos, mas também impulsionou as sociedades em direção à liberdade.

É apenas um pequeno exagero dizer que a Revolução Americana poderia não ter ocorrido se os colonos não tivessem exigido o direito à privacidade pessoal e de propriedade. A privacidade é um princípio e uma virtude revolucionária que levou os colonos americanos a fechar a porta na cara das autoridades britânicas, literal e figurativamente. A Terceira Emenda da Constituição dos EUA, por exemplo, proíbe a prática então generalizada de alistar soldados à força em residências particulares, mesmo em tempos de paz. A Emenda soa antiquada aos ouvidos modernos, mas a violação foi importante o suficiente para que os revolucionários a colocassem em terceiro lugar na lista de liberdades declaradas pela Declaração de Direitos. A Terceira Emenda afirma o direito à privacidade contra a intrusão do estado no mais pessoal de todos os reinos: o lar. Por mais ultrapassada que essa emenda possa parecer, não é necessário um grande salto para aplicar seu princípio ao atual ataque contra todas as outras formas de privacidade.

A Quarta Emenda também afirma a privacidade. Começa defendendo "[o] direito do povo à segurança de suas pessoas, casas, papéis e pertences contra buscas e apreensões irrazoáveis". Em termos de privacidade, a palavra importante é "papéis", porque pode ser extrapolada para se aplicar a e-mails e outros dados de computador, incluindo identidades reais.

A Quinta Emenda defende a privacidade ao decretar o direito de um indivíduo *de não* prestar "testemunha contra si mesmo" em casos criminais.

No linguajar do século XVIII, quando o estado vigia computadores e contas de cripto, ele está realizando uma apreensão de "papéis". No entanto, as regras de provas físicas nem sempre se aplicam de forma clara às provas digitais, e as decisões inconsistentes dos tribunais sobre privacidade das criptos causam confusão. A compreensão da crescente confusão legal sobre privacidade pode estar na palavra da Quarta Emenda – "papéis". A Emenda afirma que tanto "papéis quanto pertences [estão protegidos] contra buscas e apreensões irrazoáveis". Mas o direito consuetudinário, no qual se baseia a jurisprudência ocidental, tende a conceder maior proteção aos "papéis" do que aos "pertences", talvez porque os documentos sejam vistos como uma violação da pessoa e não da propriedade.

O professor de direito Donald A. Dripps abre seu ensaio pioneiro "'Dearest Property': Digital Evidence and the History of Private 'Papers' as Special Objects of Search and Apprehension" com duas perguntas. "Por que a Quarta Emenda se refere distintamente a 'papéis' antes de 'pertences'? Por que devemos nos importar?" Dripps pede para "fundar regras especiais da Quarta Emenda para evidências digitais" dentro da lei estatal para restringir "o volume de informações inocentes e íntimas que devem ser expostas [ou exigidas] antes que o material criminal seja descoberto". Mais uma vez, a Revolução Americana fornece uma visão.

Na década de 1760, os mandados britânicos para documentos começaram a ser emitidos contra autores e editores coloniais suspeitos de sedição. *Entick V. Carrington* (1765) é provavelmente o caso jurídico mais influente da época. Os fatos básicos do caso: John Entick publicou um jornal que se opunha à Coroa. Em 1762, oficiais invadiram a casa de Entick e roubaram centenas de papéis em busca de evidências de traição. Entick processou. Entick ganhou. O juiz presidente, Lorde Camden, ofereceu um famoso ditado: "Se for lei, será encontrado em nossos livros. Se não for encontrado aqui, não é lei". O suposto direito do estado de apreender papéis não estava nos estatutos, portanto, não era lei.

A análise subsequente do caso *Entick* descobriu que quatro aspectos do ataque do estado eram legalmente desagradáveis; todos eles se aplicam à atual vigilância e apreensão de informações financeiras. O mandado foi *indiscriminado*. A apreensão expropriou os papéis, negando seu uso ao autor. O mandado foi desregulado porque não havia supervisão neutra ou via de apelação. A apreensão foi *inquisitorial* porque deu ao estado informações sobre o funcionamento privado da mente de Entick. O advogado de Entick declarou: "Nenhuma potestade pode invadir legalmente a casa de um homem e investigá-la para buscar provas contra ele; isso seria pior do que a inquisição espanhola, pois saquear as gavetas e caixas secretas de um homem para obter provas contra ele é como torturar seu corpo para descobrir seus pensamentos secretos." A apreensão de papéis era um ataque contra a pessoa, não contra a propriedade.

Qualquer juiz que posteriormente considerasse emitir um mandado de busca de documentos tinha que considerar a decisão de Lorde

Camden: de que uma suposta ofensa precisava estar nos livros de estatuto para que existisse na lei. Além disso, mandados sobre documentos cada vez mais entravam em conflito com as constituições estaduais.

A guerra muda as leis, especialmente as leis que protegem os direitos individuais. Dripps continua: “A América se recusou a modificar a proibição da lei comum por estatuto até a Guerra Civil”. O imposto de consumo era a principal fonte de financiamento do governo federal para a guerra, mas a evasão fiscal era desenfreada. Em resposta, um estatuto único foi aprovado. “[Este] ato de 1863 foi o primeiro ato neste país […] ou na Inglaterra, até onde pudemos apurar, que autorizou a busca e apreensão de documentos particulares de um homem, ou a produção compulsória deles, para usá-los como prova contra ele em um processo criminal, ou em um processo para executar o confisco de seus bens”. A apreensão de papéis estava agora nos estatutos.

A questão dos papéis versus pertences ziguezagueou juridicamente após a Guerra Civil. Indiscutivelmente, a mudança mais importante ocorreu em 1886, quando o *Boyd v. United States* foi decidido pela Suprema Corte dos EUA. “A história do caso Boyd”, escreve Dripps, “começa corretamente com um estatuto que autoriza os funcionários da alfândega a apreender os livros e papéis de importadores suspeitos de evasão de impostos”. A Suprema Corte decidiu a favor de Boyd, dizendo:

> “Os princípios estabelecidos neste parecer afetam a própria essência da liberdade e da segurança constitucionais. Aplicam-se a todas as invasões por parte do estado e seus funcionários à santidade da casa de um homem e das privacidades da vida. Não é o arrombamento de suas portas e o remexer de suas gavetas que constitui a essência da ofensa, mas sim a invasão de seu direito irrevogável de segurança pessoal, liberdade pessoal e propriedade. É a invasão desse direito sagrado que fundamenta e constitui a essência do julgamento de Lord Camden.”

A decisão de *Boyd* restabeleceu maior proteção constitucional aos papéis do que aos pertences, e incide diretamente sobre os papéis digitais. A proteção nunca foi absoluta, no entanto, e foi severamente cor-

rompida. Dripps explica: “Durante o último quarto do século XX, a Suprema Corte começou efetivamente a equiparar ‘papéis’ e ‘pertences’. Outra linha de casos modernos estabeleceu regras de ‘linhas-claras’, que deram o mesmo tratamento constitucional a todos os ‘pertences’”. Os papéis não apenas perderam seu status especial sob o direito comum e constitucional, mas também chegaram mais perto de se tornarem legalmente intercambiáveis com todos os outros pertences. Isso oferecia uma proteção muito mais fraca. No entanto, o precedente de *Boyd* prevaleceu por quase um século e ainda não envelheceu.

A importância dos papéis está intrinsecamente ligada ao valor da privacidade para os indivíduos. Quando o estado rouba dados, não viola “propriedades” no sentido legal da palavra; ele viola a pessoa.

A privacidade faz parte de uma vida saudável, criativa e autorreflexiva. Desde a infância mantenho um diário no qual coloco esperanças, confusões, decepções e desejos. Quando leio páginas do passado, me conecto visceralmente com quem eu era aos dez anos e entendo melhor a pessoa que sou hoje. Esses diários são privados, não porque eu tenha vergonha deles, mas porque são *pessoais*. Em seu romance distópico 1984, George Orwell enfatiza a importância dos diários:

> “A única coisa que ele estava prestes a fazer era abrir um diário. Isso não era ilegal (nada era ilegal, já que não havia mais leis), mas se detectado era razoavelmente certo que seria punido com a morte.”

O protagonista de *1984* descobre seu individualismo. Nesta jornada, o diário representa a liberdade de expressão e consciência que são essenciais para um senso de identidade – tão essencial que o estado matará por esse ato de privacidade.

Toda violação de privacidade corrói o espírito humano. Uma palavra não é dita por medo de ser ouvida; um pensamento não se forma por medo de se tornar uma palavra; um sentimento nunca é expresso e, talvez com o tempo, nem mesmo sentido. Então, um dia, o silêncio exterior torna-se interior através do hábito agora automático da autocensura. As pessoas não questionam mais. Talvez nem percebam mais que não questionam mais. Eles desenvolveram o hábito de não ser um indivíduo e, em vez disso, tornaram-se parte de uma vontade coletiva.

Todo mundo tem áreas de privacidade para proteger. Alguns usam medalhões com fotos de parentes mortos; outros abrigam um amor proibido; alguns trancam a porta para deleitar-se com um banho quente sem serem incomodados, ou escondem uma preferência sexual incomum. Todo ser humano tem o direito de traçar linhas que não prejudicam ninguém, linhas que ninguém mais deveria cruzar sem ser convidado. Bata a porta na cara de quem disser o contrário!

O foco das criptomoedas na privacidade é mais do que o desejo de reter riqueza, como geralmente é acusado. É um desejo de manter a individualidade, o espírito humano e a liberdade.

Nomes Verdadeiros e Estratégias para a Privacidade

> Todos aqueles que usaram seu conhecimento em uma tentativa de promover mudanças sociais viram a criptografia como uma ferramenta para aumentar a privacidade individual e transferir o poder das grandes instituições centrais para os seres humanos que vivem em sua órbita.
> – Paul Vigna.

O mundo precisa de um novo paradigma de privacidade porque o Estado sempre vencerá sob o velho paradigma enquanto controlar a Indústria de Identidade. A indústria consiste em muito mais do que documentos de identificação do governo e formulários a serem preenchidos. Nas últimas duas décadas, a Indústria da Identidade se expandiu para incluir triagem de aeroportos, biometria, regulações Know Your Customer, caches de dados clandestinos e vigilância em cada turno. Alastair Berg, do RMIT Blockchain Innovation Hub, observa: "Esses são apenas alguns segmentos em uma indústria que deve crescer para $16 bilhões até 2022".

O Estado não vai afrouxar o controle sobre a indústria porque a identificação é uma parte insubstituível do controle social e da acumulação de riqueza. Isso é verdade desde a era napoleônica, quando foi introduzido um cartão de identidade que prenunciava os modernos. O objetivo do ID era controlar os salários, restringindo a mobilidade dos trabalhadores que queriam se mudar para obter melhores empregos com salários mais altos. As cartas foram fundamentais para converter uma França relativamente livre em um estado policial.

O monopólio estatal de identificação precisa ser quebrado da mesma maneira que as criptos quebram o monopólio monetário. Não deve ser confrontado; ele deve ser contornado, procurando-se uma alternativa melhor. Isso não apenas afasta o Estado, mas também fornece uma alternativa de livre mercado para a necessidade humana válida de identificação. Historicamente, a identificação era uma função de livre mercado; certidões de casamento, por exemplo, eram um contrato privado entre famílias e honrados pela igreja. Pode facilmente ser uma função do livre mercado novamente. Enquanto a Indústria da Identidade

for um ramo do governo, no entanto, essa necessidade humana ficará insatisfeita ou será satisfeita a um custo assombroso para a liberdade.

O novo paradigma online para privacidade está aqui. É exemplificado pela blockchain onde as interações são transparentes e as identidades reais são protegidas. A privacidade reside na proteção de True Names (Nomes Verdadeiros) – uma referência à novela pioneira de 1981, de Vernor Vinge, na qual um grupo de hackers (chamados warlocks/feiticeiros) invade computadores ao redor do mundo. Suas identidades reais são secretas umas das outras e especialmente do Grande Adversário – uma referência ao estado americano. Mascarar identidades do mundo real é vital porque qualquer um que conheça o True Name de um "feiticeiro" pode chantageá-lo ou causar uma True Death (Morte Verdadeira). A identidade é literalmente uma questão de vida ou morte.

A origem dos True Names

> "Acho que o carteiro está nos atacando um de cada vez, começando com os mais fracos, nos atraindo o suficiente para aprender nossos Nomes Verdadeiros – e então nos destruindo."
> – Vernor Vinge, *True Names*

True Names é uma das primeiras representações ficcionais de um ciberespaço desenvolvido. É amplamente creditado como iniciador do movimento cyberpunk, que mais tarde explorou muitos dos temas apresentados na novela.

A novela começa da seguinte maneira:

> Nos dias de era-uma-vez da Primeira Era da Magia, o feiticeiro prudente considerava seu próprio nome verdadeiro como seu bem mais valioso, mas também a maior ameaça à sua vida, pois – as histórias contam – uma vez um inimigo, mesmo um inimigo fraco e não qualificado, aprendeu o verdadeiro nome do feiticeiro, e então feitiços rotineiros e amplamente conhecidos poderiam destruir ou escravizar até mesmo os mais poderosos. Com o passar dos tempos, chegando à Idade da Razão, e daí para a primeira e a segunda revoluções industriais, tais noções foram desacreditadas. Agora parece que a Roda deu uma volta completa (mesmo

> que nunca tenha havido realmente uma Primeira Era) e voltamos a nos preocupar com nomes verdadeiros novamente.

Na história, o hacker protagonista é visitado por agentes do Grande Inimigo que descobriram seu Verdadeiro Nome. Eles o armam para rastrear um alvo maior conhecido como The Mailman. Assim, a história é altamente antiestatista com um senso aguçado de como a identidade é crucial para a liberdade.

A novela despertou a admiração dos criptoanarquistas, que também se basearam em sua visão do ciberespaço. Uma reimpressão posterior de *True Names* inclui dez artigos e ensaios de escritores que fornecem comentários sobre a história de Vinge. Um deles é o ensaio "True Nyms and Crypto Anarchy" de Timothy May, autor de "The Crypto Anarchist Manifesto". (Nyms é a abreviação de pseudônimos.) No tributo a *True Names,* May afirma com otimismo:

> "A criptoanarquia é a realização ciberespacial do anarcocapitalismo, transcendendo as fronteiras nacionais e liberando os indivíduos para fazer consensualmente os arranjos econômicos que desejam fazer."
> Isso garante que homens com armas não possam ser trazidos para interferir em transações mutuamente acordadas, o único tipo de interação econômica possível na anarquia criptográfica. Algumas pessoas, é claro, gritarão: "Injusto!", e exigirão a intervenção do governo, razão pela qual a criptografia pesada provavelmente sofrerá oposição das massas, a menos, é claro, que as massas sejam sábias e tenham uma visão de longo prazo. Isso pode cheirar a elitismo, mas tenho muito pouca fé na democracia. De Tocqueville alertou em 1840 que, traduzido aproximadamente: "A República Americana durará até que os políticos percebam que podem subornar as pessoas com seu próprio dinheiro". Chegamos a esse ponto há várias décadas.

A criptografia pesada e a privacidade que ela oferece são essenciais para o sucesso da criptoanarquia. Sua antítese é o controle social, que requer identificar as pessoas e vinculá-las às atividades para ser eficaz. A criptografia quebra esse vínculo. E nunca é cedo demais.

Atualmente, a identidade do governo é a única maneira pela qual a maioria das pessoas pode provar suas identidades offline para acessar as necessidades da vida moderna. Na maioria dos países ocidentais, pessoas indocumentadas não podem embarcar em um avião, dirigir um carro ou alugar um apartamento. Elas não podem abrir uma conta bancária, adquirir um cartão de crédito, acessar cuidados médicos, descontar um cheque, ter um emprego visível, frequentar uma universidade ou comprar um carro. Tornam-se cidadãos de segunda classe.

Enquanto isso, aqueles com identidade estatal tornam-se vulneráveis a processos e perseguições. Em um sistema nacionalizado de identificação e relatórios, o governo sabe quem são todos, o que cada um possui e onde encontrar ambos. Como Orwell argumenta eloquentemente em romances e ensaios, a nacionalização da privacidade é um pilar do totalitarismo. Não é de admirar que o apetite do governo por dados seja tão voraz. Não é à toa que há um esforço para retirar o anonimato da Internet sob a égide da preocupação com o bullying.

O que é necessário agora é um novo paradigma para a privacidade offline que possa funcionar em conjunto com as proteções online. Ou melhor, um velho paradigma deve ser revivido. A privacidade offline é melhor alcançada pelo ID de livre mercado, que fornece os benefícios da identificação sem a responsabilidade de se tornar um número em um arquivo burocrático.

Sistemas offline de identificação de livre mercado

A identidade de livre mercado é a antítese da identidade do governo na medida em que devolve o poder de identificação ao indivíduo para usar ou não de acordo com seu próprio critério. A identidade de livre mercado é uma aliada natural da criptografia, porque os objetivos são os mesmos – quebrar o monopólio estatal da indústria de identidade.

Quando o comércio estava no nível do escambo, as pessoas geralmente conheciam os indivíduos com quem negociavam. Quando o comércio se expandiu para incluir trocas complexas com estranhos a um mundo de distância, a troca direta foi substituída pela troca indireta, que muitas vezes exigia confiança ou um intermediário. A base da confiança em alguém é a capacidade de responder à pergunta: “Com quem estou lidando?”. Assim, há uma necessidade legítima de identificação e pouco perigo para ela enquanto o estado não estiver envolvido.

Considere um método difundido de identificação de séculos atrás que está voltando – cartas de apresentação. A dinâmica básica: a pessoa A carrega cartas de identificação para a pessoa C a quem A é um estranho. As cartas são escritas pela pessoa B, que é um conhecido respeitado e mútuo. A pessoa B atesta a identidade do portador da carta e C é capaz de responder à pergunta: "Com quem estou lidando?". Essas cartas podem ser preparadas por uma empresa que verifica identidades para obter lucro.

Uma versão eletrônica de cartas de apresentação ocorre em círculos de criptografia e em redes sempre que um membro respeitado atesta um estranho que deseja participar. Dado o tamanho da comunidade e o fato de estar sob ataque, as introduções parecem ser uma prática cada vez mais popular.

As cartas incorporam o primeiro e mais básico serviço prestado pelo ID do livre mercado: a *autenticação*. Existem inúmeras razões pelas quais alguém gostaria de autenticar a identidade de uma pessoa. A pessoa pode estar pegando um pacote, confirmando uma reserva, ingressando em um clube, descontando um cheque ou solicitando um emprego. O filtro de autenticação significa que um estranho não pode cometer fraudes.

A autenticação no livre mercado de identidades reais também pode ser realizada por empresas que emitem carteiras de identidade. A identificação privada é comum hoje em uma forma bastarda que tem valor limitado. Os empregadores emitem IDs aos funcionários para que possam desbloquear escritórios; as instituições financeiras oferecem cartões de crédito aos clientes; as universidades distribuem carteiras de identidade para que os alunos possam acessar os serviços. Mas a privacidade aqui é ilusória. Antes que um empregador ou uma instituição financeira emita o ID, o destinatário é selecionado no processo de contratação ou na abertura de uma conta. Os cartões de estudante são pré-selecionados pela extensa documentação necessária para se matricular em uma universidade. Esta informação é rotineiramente relatada ao estado de uma forma ou de outra. Esses IDs semiprivados podem ser uma prova de princípio, mas não são de livre mercado ou privados.

A agorista Sunni Maravillosa especula sobre como seria a identidade de livre mercado em seu ensaio "ID without Big Brother", na antologia *National Identification Systems: Essays in Opposition*:

> "Se um indivíduo deseja um documento de identidade que atribua um determinado rótulo a ele, ele tem várias empresas para escolher. IDs R Us é uma rede nacional que possui requisitos mínimos para tal identificação, e oferece atendimento rápido a preços baixos. No entanto, por ter requisitos mínimos, seu histórico de segurança não é tão bom e muitas empresas não confiam muito em seus IDs. O emissor de ID de autenticação mais bem-sucedido é o Spooner's Identity Emporium. Essa empresa também tem requisitos mínimos para identificação apenas de nome de baixo nível, mas dá a etapa adicional de verificar o histórico do candidato à identificação com esse nome, bem como a reputação daqueles que garantem o candidato à identificação. A empresa publica uma lista mensal em seu site – geralmente uma lista muito curta, devido ao seu processamento cuidadoso – de indivíduos cuja identidade foi revogada, juntamente com o motivo da revogação [...] Claro, se um indivíduo não gostar dos requisitos de uma empresa, ela está livre para usar outra [...]"

A maioria das empresas teria cuidado com a precisão porque qualquer pessoa fraudada por um documento falso pode entrar com uma ação legal. Eles também teriam cuidado com a privacidade do cliente, pois a discrição seria a chave para a comercialização de seu ID. Se os IDs emitidos pela empresa facilitarem a fraude ou se as informações do cliente vazarem, a publicidade por si só prejudicaria ou arruinaria a reputação da empresa; as empresas de identidade de livre mercado viveriam e morreriam com base em suas reputações.

O segundo serviço que a ID de livre mercado oferece aos indivíduos é a *certificação*. Cartas de recomendação atestam o caráter, a educação e as habilidades específicas do portador. As empresas provavelmente cooperariam umas com as outras no fornecimento de tais cartas. Maravillosa oferece um exemplo hipotético:

> Os bancos emitem "credenciais de crédito", que se baseiam no histórico de crédito de um indivíduo ou empresa com o banco, para que outro indivíduo ou instituição esteja con-

vencido de que a entidade em questão é diferente de inadimplência em um empréstimo ou outro acordo de crédito até um determinado valor.

Novamente, a versão cripto desse serviço é uma recomendação online pessoal de uma figura confiável sobre um estranho. Alternativamente, o estranho poderia apontar para documentos de certificação – talvez artigos acadêmicos que ele escreveu sobre assuntos relevantes. Sua própria reputação pode ser uma identificação de certificação.

Algumas formas de ID atual executam uma função semelhante. Os diplomas universitários supostamente certificam um nível de educação e inteligência; uma carta de referência de um empregador descreve os hábitos de trabalho louváveis de um ex-funcionário; a participação em organizações profissionais ou de caridade sugere o caráter e as habilidades sociais de uma pessoa.

Há uma desvantagem marcada para muitas certificações atuais, no entanto. Uma delas: as licenças e diplomas estatais frequentemente substituem os métodos de certificação do livre mercado. Tudo, de neurocirurgia a tranças de dreadlocks, exige licenças, e estas tendem a substituir a reputação como medida de valor. Um exemplo: Um curandeiro não tradicional é bem conhecido por sua habilidade, mas não consegue obter uma licença. Sua reputação é gigantesca, mas os médicos locais bloqueiam o processo de licenciamento para eliminar a concorrência. O curandeiro é incapaz de tratar as pessoas sem o risco de ir para a cadeia. Diplomas exigidos pelo estado – mesmo que tenham valor, o que é cada vez mais duvidoso – são barreiras para aqueles que são talentosos, mas não sancionados pelo estado. Desta forma, o estado desvaloriza ou nega o valor da reputação.

O terceiro propósito da ID de livre mercado é *autorizar* ações específicas. As cartas podem atribuir direitos limitados ao portador. Um escritório de advocacia pode atribuir um poder limitado a um de seus advogados para que ele possa resolver um caso em nome de um cliente.

Objeções ao ID de livre mercado

Surgem objeções à identificação de livre mercado. Diz-se que os métodos de identificação são antiquados, não fornecem anonimato real

e não têm uniformidade. Além disso, estabelecer uma reputação é um processo lento em um mundo em rápida evolução.

Antiquado. Alguns modelos de identificação podem estar ultrapassados. Mas o remédio mais seguro para isso é abrir o campo e deixar o mercado inovar. Os IDs mais antiquados são os produzidos pelo estado estagnado.

Sem anonimato. O objetivo principal da identificação inicial era verificar a identidade, não tornar o anonimato. E ainda há uma demanda de livre mercado para verificar a identidade. Há valor no anonimato; há valor em ser conhecido. O valor depende de se o indivíduo é capaz de escolher livremente entre os dois.

Sem uniformidade. Outra palavra para "sem uniformidade" é "diversidade", e é uma das vantagens extremas do ID de livre mercado porque dá escolha. A identidade do governo é homogeneizada porque o objetivo é impor a conformidade com as leis e os requisitos de relatórios. Quando o ID atende a indivíduos, sua forma é ditada por suas necessidades e preferências, não pelo estado.

Lento para estabelecer confiança ou reputação. Este é um mundo corrido. Mas o fato de que uma reputação ou um negócio pode levar tempo e trabalho duro para se estabelecer dificilmente é uma crítica. Conquistas que valem a pena levam tempo e trabalho duro.

A opção nuclear do estado no armamento de dados

> "A privacidade inclui a capacidade de manter as coisas em segredo do governo. Posso estar mantendo em segredo minha fraqueza por álcool, heroína, jogos de azar ou pornografia e, assim, impedir que o governo interfira para me proteger de mim mesmo. Se você vê o governo como um super ser benevolente cuidando de você – um tio sábio e gentil com uma longa barba branca – você vai e deve rejeitar muito do que estou dizendo. Mas o governo não é o Tio Sam ou um rei filósofo. O governo é um conjunto de instituições através das quais os seres humanos agem para fins humanos. Sua característica especial – o que diferencia a ação política das outras maneiras pelas quais tentamos obter o que queremos – é que o governo pode usar a força para fazer as pessoas fazerem coisas."
> – David Friedman

O governo não é um tio sábio e gentil. É uma instituição de interesse próprio ocupada por seres humanos com paixões humanas, especialmente por poder, riqueza, status, moralização e vingança. Atualmente, os usuários de cripto têm motivos para serem particularmente privados. Uma notícia recente declara: “A NSA rastreia usuários de Bitcoin desde 2013, novos documentos de Snowden são revelados”. Muita cautela tanto online quanto offline não é paranoia quando eles de fato estão atrás de você.

Uma manchete de 6 de fevereiro de 2018 na revista *Reason* alerta: “Os governos odeiam Bitcoin e dinheiro vivo pelo mesmo motivo: eles protegem a privacidade das pessoas”. O artigo a seguir deriva de uma citação do secretário do Tesouro dos EUA, Steve Mnuchin: “Uma das coisas em que trabalharemos muito de perto com o G-20 é garantir que isso não se torne as contas bancárias numeradas na Suíça”. Mnuchin rejeita as criptos descentralizadas como sistema de pagamento, investimento ou poupança porque não podem ser facilmente rastreadas pelo governo. A crítica de Mnuchin confirma que as criptomoedas são um bem positivo para os indivíduos, não apenas porque os empodera, mas também porque os protege de estatistas como ele.

Os ataques de privacidade em todo o mundo ficarão rapidamente mais agressivos. Os dados estão sendo transformados em armas em um ritmo assustador, criando uma corrida acirrada entre privacidade e totalitarismo. Estados estão desenvolvendo novas maneiras de usar bancos de dados para reprimir as oportunidades e atividades de pessoas que fazem escolhas “erradas” ou que têm pensamentos “errados”.

Uma manchete na Reuters dizia: “China barrará pessoas com mal ‘crédito social’ de aviões e trens”. O crédito social (*xinyong*) é um conceito moral de longa data dentro da tradição chinesa, que indica o nível de honestidade e confiabilidade de uma pessoa. O governo chinês agora estende esse conceito moral para incluir lealdade ao estado e honestidade social ou política; atribui uma classificação oficial a cada pessoa. Então, o controle social extremo é imposto àqueles com pontuações baixas, negando-lhes “privilégios”, como viagens e educação. Os crimes de crédito social incluem usar bilhetes vencidos para embarcar em um trem ou fumar enquanto estiver nele, comprar muito álcool, assistir pornografia, devolver uma bicicleta alugada com atraso, “não comparecer a um restaurante sem cancelar a reserva, trapacear em jogos online, deixando avaliações falsas de produtos, e atravessar a rua fora da faixa.”

As ofensas triviais podem parecer intrigantes ou até engraçadas, mas servem a um propósito importante para o Estado e horripilante para os indivíduos. As ofensas triviais dão ao Estado um cheque em branco para reprimir dissidentes, opositores políticos ou outros "indesejáveis", porque praticamente todos cometem infrações menores como parte da vida cotidiana. Como Beria disse uma vez: "Mostre-me o homem, eu lhe mostrarei o crime". O governo chinês agora pode escolher quem deseja converter em não-pessoa, impedindo-os de viajar e outras interações sociais. A estratégia é semelhante à descrita no livro *Three Felonies a Day*, segundo a qual todos que violam a autoridade do estado são vulneráveis a acusações criminais por um ou outro delito. Todo mundo é vulnerável aos ataques do estado. Esse perigo também fornece um grande incentivo para que as pessoas obedeçam absolutamente e não chamem a atenção para si mesmas. Isso é verdade na China. É cada vez mais verdade em muitas nações.

O conceito de crédito social não é exclusivamente chinês. Nos EUA, os passaportes são negados àqueles que estão suficientemente atrasados no pagamento de pensão alimentícia ou de impostos, e ex-criminosos têm dificuldade em viajar para o exterior. Os estrangeiros que disserem a um guarda de fronteira dos EUA que fumaram maconha, independentemente de o evento ter ocorrido em um local onde era legal ou não, terão sua entrada recusada. *Global News*, um portal de notícias canadense, explica: "eles são […] instruídos a voltar para o Canadá e informados de que são inadmissíveis pelo resto da vida. Esta é uma proibição vitalícia." Enquanto isso, direitos constitucionais como a posse de armas estão sendo negados por uma lista cada vez maior de razões.

O apetite voraz do governo pelos dados exigidos pelo controle social está crescendo. O Cloud Act tornou-se lei federal em 2018, por exemplo. A lei permite que a aplicação da lei federal obrigue as empresas de tecnologia sediadas nos EUA a fornecer dados armazenados em servidores, independentemente de onde os dados estão armazenados. Ele retira os direitos da Quarta Emenda contra busca e apreensão irracionais, permitindo que os EUA celebrem acordos de compartilhamento de dados com países estrangeiros e ignorem os tribunais dos EUA. Os usuários-alvo podem nunca saber do mandato.

As pessoas precisam escolher sua abordagem à privacidade e se preparar.

O que você deveria fazer?

As estratégias variam de pessoa para pessoa, porque são baseadas em variáveis como personalidade e circunstância. Existem muitos caminhos para a privacidade, não apenas um.

Antes de responder "O que você deve fazer?", algumas distinções são úteis. Todas as informações não são iguais, e criptografar tudo pode chamar atenção indesejada. Você pode considerar criptografar apenas informações importantes para sua liberdade, riqueza e bem-estar. Todo mundo tem pelo menos três tipos de dados pessoais. Primeiro, há dados que devem ser amplamente divulgados, como um currículo de emprego. Esta informação requer marketing, não privacidade. Em segundo lugar, há fatos que são inofensivos de divulgar, como uma cor favorita ou uma preferência por batatas fritas. A divulgação pode atrair solicitações indesejadas de negócios, mas esses aborrecimentos não comprometem direitos. Terceiro, há fatos que os maus agentes podem usar contra você. Os dados financeiros são um excelente exemplo. Este é o ponto em que a privacidade se torna um mecanismo de sobrevivência.

A próxima distinção é o terreno bem trilhado da privacidade versus anonimato versus pseudônimo. Vou pisar nessa questão mais uma vez e brevemente.

Privacidade é o ato de manter dados pessoais ou atividades para si mesmo em sua totalidade ou para qualquer que seja o seu nível de conforto. Qual é o seu nível de conforto?

O anonimato é a estratégia de tornar o conteúdo transparente, mas ocultar os Nomes Verdadeiros. Rick Falkvinge, fundador do primeiro Partido Pirata, elabora:

> "O exemplo típico seria se você deseja denunciar abuso de poder ou outras formas de crime em sua organização sem arriscar a carreira e a posição social desse grupo, e é por isso que normalmente temos leis fortes que protegem as fontes da imprensa livre. Você também poderia postar esses dados anonimamente online por meio de uma VPN, da rede de anonimização TOR ou de ambos. Este é o equivalente análogo da carta de denúncia anônima, que tem sido vista como um procedimento padrão em nossas checagens e avaliações."

O pseudônimo é a estratégia de usar um nome fictício em vez de um Nome Verdadeiro. É o anonimato adquirido pelo disfarce. A pseudonimidade não é um fenômeno recente. Os influentes *The Federalist Papers* (1787-1788) foram escritos por Publius – um pseudônimo coletivo que abrange James Madison, Alexander Hamilton e John Jay. Os historiadores ainda discordam sobre quem escreveu algumas das peças; isso atesta a eficácia do pseudônimo.

As táticas mais eficazes para proteger dados online podem ser tecnológicas, mas este livro não as aborda, exceto de passagem. Em vez disso, ele aponta para estratégias ou hábitos de privacidade que são usados há décadas, se não há séculos. Alguns deles serão familiares. O objetivo não é promover material novo ou revolucionário; é conscientizar as pessoas a pensar em como manter a privacidade.

Eles foram atualizados para focarem nas criptomoedas. Aqui está uma amostra de algumas técnicas básicas e eficazes:

Ofuscar ou "esconder à vista de todos". Seja tão discreto ou sutil em suas ações externas e aparência que seja quase imperceptível. Misture-se e torne-se invisível. Às vezes, a ofuscação envolve a participação em locais tão cheios de "ruído" que um bisbilhoteiro acha difícil distinguir seu sinal de qualquer outro. O cerne desta estratégia é evitar chamar atenção para si mesmo. Quando você fizer coisas "notáveis", como pedir a derrubada do sistema bancário central, faça-o sob um pseudônimo. Sob seu Nome Verdadeiro, seja cauteloso.

Evite corretoras centralizadas e outros centros de compartilhamento de dados. Esta é uma versão atualizada para usuários de cripto do conselho de evitar centros de coleta de dados conectados ao estado, como os bancos centrais. Se você deseja que o estado tenha todos os seus dados financeiros, basta enviá-los por correio para as agências estaduais.

Proteja tudo com senha e fique livre de vírus. Uma senha é como uma fechadura em uma porta que dificulta a entrada de malfeitores. Evite vírus e malwares através dos quais hackers podem atacar seus dados e roubar sua identidade. Nunca abra arquivos não solicitados em e-mails; nunca baixe arquivos de sites desconhecidos ou inseguros. Execute um programa antivírus competente e prefira navegadores que resistam a penetrações, como os usados em Linux.

Encontre maneiras discretas de sacar. O veterano das criptos Kai Sedgwick escreve: "As transações Bitcoin são semianônimas: todas as transações na blockchain são transmitidas publicamente e visíveis por

toda a eternidade, mas o proprietário de cada carteira é desconhecido. Vincular endereços a identidades do mundo real agora é relativamente fácil para os poderosos, porque todos precisam sacar em algum lugar, e isso geralmente envolve vincular endereços de Bitcoin a contas bancárias." Não use terceiras partes confiáveis para sacar. Na medida do possível, lide com as pessoas individualmente ou por meio de corretoras descentralizadas que facilitam a compra e a venda peer-to-peer. Seja inventivo. Procure locais que troquem criptomoedas por gift-cards em lojas nas quais você faz compras regularmente, incluindo mercearias.

Escolha um mecanismo de pesquisa que respeite a privacidade. Muitos mecanismos de pesquisa registram históricos de navegação e os usam para segmentar anúncios ou gerar receita vendendo-os. Outros, como o DuckDuckGo, não rastreiam dados pessoais.

Use uma moeda de privacidade. Existem dezenas dessas moedas e mais estão chegando porque a privacidade está em demanda. O fundador da Zcash explica a filosofia por trás de sua moeda de privacidade. "Acreditamos que a privacidade fortalece os laços sociais e as instituições sociais, protege as sociedades contra seus inimigos e ajuda as sociedades a serem mais pacíficas e prósperas [...] Uma tradição robusta de privacidade é uma característica comum em sociedades ricas e pacíficas, e a falta de privacidade é frequentemente encontrada em sociedades com dificuldades e fracassadas".

Nunca dê mais informações do que o necessário. Nunca forneça informações, especialmente por escrito, sempre que a recusa ou o silêncio for uma opção. Se um formulário é obrigatório, preencha o menor número de espaços em branco possível da forma mais confusa possível. Desconfie de qualquer empreendimento conectado às criptomoedas que exija mais do que informações mínimas para adquirir o serviço ou bem que está sendo oferecido. Ninguém nas criptos precisa saber seu número de previdência social, mesmo os últimos quatro dígitos. Sempre pergunte a quem solicita informações "por que" elas são necessárias e quais os usos que farão delas. Decida com antecedência quantos dados você está disposto a divulgar e de que forma.

Seja cauteloso em fóruns públicos. Fóruns públicos, como Facebook ou Twitter, são monitorados e explorados por governos e corporações; eles também são monitorados por criminosos e pessoas maliciosas que guardam rancor. Fóruns públicos são pontos de coleta de dados pessoais, mesmo que uma pessoa pense que está postando anonimamente.

Se a mídia social for necessária por motivos profissionais, use-a ao mínimo e apenas por motivos profissionais. Nunca publique nada nas redes sociais que você não colocaria na primeira página do *New York Times*.

Tenha cuidado ao registrar informações. Não anote chaves privadas, por exemplo, sem ter um local seguro e não divulgado para armazená-las. Não faz sentido criptografar dados online se o mesmo informativo estiver em forma cursiva na mesa da cozinha.

Use apenas conexões Wi-Fi seguras. É comum as pessoas se conectarem ao Wi-Fi gratuito na Starbucks e em outros locais, mas não há como saber quem pode estar ouvindo seu tráfego de internet. Se você precisar usar Wi-Fi inseguro, não transmita dados pessoais e use um serviço VPN para criptografar dados pessoais.

Minta ao estabelecer perguntas de segurança de senha. "Qual é o nome de solteira da sua mãe?" Com essas informações, alguém malicioso pode invadir suas contas bancárias e, talvez, roubar sua identidade. Não responda a esta ou a outras perguntas de "identificação" padrão com sinceridade. Tenha uma resposta falsa padrão que você não use em formulários oficiais ou importantes que sejam seguros. Sobre esses, diga a verdade.

As precauções rudimentares anteriores destinam-se a formar o hábito da privacidade. Muitas pessoas têm o hábito de revelar, de dizer a verdade reflexivamente. Um hábito nada mais é do que uma resposta automática que resulta de um padrão de comportamento estabelecido. Pode ser difícil quebrar o hábito da divulgação e substituí-lo pela discrição, mas é necessário fazê-lo. Nunca minta para um amigo, mas não entregue a um estranho as chaves da sua identidade.

O governo está indo atrás das criptos, o que significa que ele está investigando os usuários. Seu ataque na linha de frente será um ataque à privacidade, porque a privacidade é a espinha dorsal da criptografia como ferramenta de liberdade. Agora é a hora de aumentar a vigilância. Parafraseando a comediante Lily Tomlin: "Não importa o quão paranoica eu fique, nunca é suficiente para acompanhar o ritmo".

A privacidade pode ser a defesa da linha de frente da liberdade individual, mas a descentralização é a condição social sob a qual a privacidade prospera. Ninguém pode ou deve dizer aos indivíduos qual estratégia específica usar. Mas, se você valoriza privacidade e segurança, mantenha a privacidade e se descentralize.

SEÇÃO TRÊS

Descentralização

Descentralização no Núcleo da Cripto-Liberdade

> “Muitas pessoas descartam automaticamente a moeda eletrônica como uma causa perdida por causa de todas as empresas que faliram desde a década de 1990. Espero que seja óbvio que foi apenas a natureza centralmente controlada desses sistemas que os condenou. Acho que esta é a primeira vez que estamos tentando um sistema descentralizado e não baseado em confiança.”
> – Satoshi Nakamoto

Apesar do incrível sucesso das criptomoedas, a questão de saber se o livre mercado pode estabelecer um sistema monetário viável ainda surge. Muitas vezes é sugerido que a cripto é viável apenas porque existe em paralelo com a moeda fiduciária, com a qual é conversível e sobre a qual se baseia. Mas será que a instituição do dinheiro, em última análise, exige supervisão confiável de terceiras partes e o envolvimento do estado? (Uma instituição é uma lei, prática ou costume estabelecido dentro de uma sociedade).

A questão pode ser reduzida a uma mais fundamental: como surge qualquer instituição dentro da sociedade e como ela declina? A resposta está dentro dos conceitos de descentralização e centralização.

O que é Centralização? O que é Descentralização?

A centralização concentra o controle de uma atividade ou organização sob uma única autoridade para coordenar os resultados. Em termos de monopólio monetário, a atividade é a sociedade; a autoridade é o estado que coordena o fluxo de finanças com o objetivo declarado de produzir uma economia eficiente e produtiva. Outro termo para o controle centralizado da sociedade é “engenharia social”. O estado aplica as teorias da ciência social à gestão de seres humanos para controlar o posicionamento e funcionamento de cada um. O controle social visa alcançar uma sociedade que seja justa ou efetiva de acordo com a visão dos responsáveis.

Nem toda centralização dispensa a escolha individual. Empresas privadas podem centralizar-se sob uma equipe de gerenciamento para

aumentar os lucros, por exemplo. Quando o fazem, muitas vezes são chamadas de corporações. A diferença crucial entre esse cenário e a centralização estatal é que as empresas são voluntárias e os indivíduos envolvidos são livres para ir embora e se juntar a um concorrente. Com o controle social, os indivíduos não têm escolha. Afastar-se significa infringir a lei, e não há concorrente.

A descentralização é a difusão do poder de uma autoridade central para suas unidades constituintes. Na arena política, isso significa passar o controle do nível nacional para o local. A discussão da descentralização geralmente começa e termina na esfera política, com o poder ainda investido em uma autoridade coordenadora. Um governo local pode ser melhor do que um remoto porque é mais responsivo à comunidade, mas o ponto final lógico da descentralização é o indivíduo, que é o alicerce de toda a sociedade e sua unidade constituinte mais básica. Esse arranjo é tanto um método quanto um objetivo. O método é o empoderamento do indivíduo. O objetivo é uma sociedade saudável, na qual cada membro faça suas próprias escolhas de acordo com seu próprio interesse.

A centralização está tão entrelaçada no tecido da cultura que muitas pessoas acreditam ser necessária para o funcionamento da sociedade. Escolas públicas, bancos centrais, sistema judiciário, obras públicas, estradas governamentais, tarifas … A maioria das pessoas não consegue visualizar a sociedade através de qualquer outra lente que não a do controle estatal centralizado; é tudo o que conhecem e tudo o que aprenderam.

Ao longo da maior parte da história, a sociedade foi vista como o resultado do projeto de alguém. O designador pode ser Deus, um chefe tribal, um monarca, um comitê de socialistas ou comunistas, uma equipe de especialistas ou alguma outra entidade que também era o estado, só que com outro nome. A sociedade era vista como uma construção artificial criada e gerida pelas autoridades. A sociedade era considerada dependente de uma autoridade coordenadora para sua lei, moralidade e prosperidade.

Em sua obra de três volumes *Law, Legislation and Liberty*, o teórico social Friedrich Hayek se refere a essa posição como “racionalismo construtivista”. Uma crença construtivista central é que o homem pode e deve inventar conscientemente instituições sociais, como a lei, através da aplicação da razão e da ciência social. Hayek argumenta vigorosamente contra essa perspectiva, alegando que os construtivistas não compreendem o processo pelo qual as instituições da sociedade surgem e

evoluem. De fato, ele acredita que a abordagem construtivista é antitética com o processo real, e dificulta as instituições sociais que deveriam evoluir em vez de seguir um plano. Em uma palestra no Memorial do Nobel de 1974 intitulada "The Pretense of Knowledge", Hayek expressa uma objeção epistemológica básica ao construtivismo – isto é, uma objeção baseada em uma teoria do conhecimento humano. Ele afirma que nenhum comitê pode predizer as escolhas em evolução e os resultados não intencionais de uma massa de pessoas que interagem ao longo do tempo. A preferência humana é muito variável e muda de forma a frustrar todo o planejamento.

Para reciclar uma citação anterior no livro:

> "O reconhecimento dos limites insuperáveis para esse conhecimento deve […] ensinar ao estudante da sociedade uma lição de humildade que deveria protegê-lo de se tornar um cúmplice da batalha fatal do homem para controlar a sociedade – uma batalha que não apenas o fará um tirano sobre seus semelhantes, mas que pode muito bem fazê-lo o destruidor de uma civilização a qual nenhum cérebro designou, mas sim que cresceu dos esforços livres de milhões de indivíduos."

Contemporâneo de Hayek, Ludwig von Mises chega à mesma conclusão de um ângulo menos epistemológico e mais econômico em sua obra-prima *Human Action*:

> "A ação humana origina a mudança. Na medida em que há ação humana, não há estabilidade, mas alteração incessante […] Os preços do mercado são fatos históricos expressivos de um estado de coisas que prevaleceu em um instante determinado do processo histórico irreversível. […] No imaginário e, claro, estado irrealizável de rigidez e estabilidade, não há mudanças a serem medidas. No mundo atual de mudanças permanentes, não há pontos fixos […]"

Tanto Hayek quanto Mises acreditam que o conhecimento buscado pelos construtivistas é inatingível. Não é possível planejar a dinâmica de amanhã com base na de ontem porque as preferências das pes-

soas e outras circunstâncias são imprevisíveis, mesmo pelas pessoas envolvidas; suposições são possíveis, mas o conhecimento não é. Mesmo uma coisa pequena, como o preço do pão ontem, não dá conhecimento do preço do pão amanhã, porque pode disparar devido à falta de farinha ou a uma mudança nas prioridades das pessoas.

Usar uma foto estática da sociedade de ontem para projetar o futuro vai contra um princípio básico da ação humana e da natureza humana: mudança inevitável. A mudança inevitável é uma diferença fundamental entre os seres humanos e os objetos físicos examinados pelas ciências exatas sobre as quais os construtivistas baseiam sua teoria social. Um cientista pode aprender tudo o que precisa saber para prever o comportamento de uma rocha porque a rocha é estática ao longo do tempo. A água continua a ter a mesma estrutura molecular e continua a ser definida por constantes, como a lei da gravidade, por exemplo. Mas a sociedade não consiste em objetos invariáveis. O comportamento dos seres humanos é baseado na alteração de preferências, emoções e respostas psicológicas que podem ser conflituosas ou ocultas até mesmo das pessoas que estão agindo. Os seres humanos não podem ser categorizados, empilhados e obrigados a obedecer às leis da ciência. A sociedade consiste em indivíduos imprevisíveis, que reagem a mudanças nas circunstâncias. Não são rochas ou água.

Há duas maneiras de os teóricos sociais abordarem a desobediência do homem imprevisível. Eles podem aceitar a natureza dos seres humanos e trabalhar suas teorias em torno dela, ou podem tentar mudar a natureza do homem para que ele se adeque às teorias deles.

Os construtivistas escolhem a segunda opção, com o novo Homem Soviético ou Pessoa Soviética sendo uma manifestação de suas teorias. O novo homem soviético foi considerado a evolução lógica dos seres humanos sob o regime comunista. Em seu livro *The Mass Psychology of Fascism* (1933), o psicanalista alemão Wilheim Reich pergunta: “O novo sistema socioeconômico se reproduzirá na estrutura do caráter das pessoas? Se sim, como? Suas características serão herdadas por seus filhos? Será ele uma personalidade livre e autorregulada? Os elementos de liberdade incorporados à estrutura da personalidade tornarão desnecessárias quaisquer formas autoritárias de governo?”

A natureza humana, assim como a sociedade, seria reconstruída por aqueles que estão no poder. O novo homem soviético era um arquétipo ou ser humano ideal com características específicas que seriam pro-

jetadas e que evoluiriam a partir do comunismo. A nova natureza humana seria compartilhada por todos os povos soviéticos, independentemente de fatores como diferentes origens culturais ou étnicas. As características comunistas incluíam altruísmo, entusiasmo pelo comunismo, saúde física, coletivismo e disciplina. Também haveria uma nova mulher soviética, como o mundo nunca tinha visto antes – abnegada e dedicada aos ideais revolucionários.

Em contraste, Hayek trabalha desapaixonadamente com a natureza humana como ela se mostra a ele: interessada por si mesma e individualista. Ele vê a engenharia social como sendo mais que meramente impossível: é também tremendamente destrutiva, porque é a antítese de uma sociedade natural e destrói as instituições liberais que evoluíram para servir aos indivíduos, e não ao estado.

Hayek conhecia em primeira mão as terríveis consequências do planejamento central. Ele havia testemunhado a devastação do liberalismo clássico por duas guerras mundiais, mas especialmente pela Primeira Guerra Mundial, que despedaçou os moldes do livre mercado. O governo em tempo de guerra havia fixado o controle centralizado sobre o setor privado para garantir o fluxo de armamentos e outros bens “necessários”. O dinheiro havia sido drasticamente inflacionado e reduzido em valor para pagar por maciços aumentos militares. A guerra estrangulou o fluxo do livre comércio, que os liberais clássicos pensavam ser um pré-requisito para a paz entre as nações, bem como para a prosperidade dos indivíduos. Hayek viu como a máquina centralizadora do estatismo do século XX destruiu a promessa do liberalismo clássico do século XIX.

Em refutação ao construtivismo, os economistas austríacos descrevem como as instituições em uma sociedade saudável surgem espontaneamente. As descrições geralmente começam com modelos simplistas para ilustrar um princípio básico ou ponto – o jeito como um caminho é forjado através de um campo, por exemplo. Uma pessoa toma o caminho mais curto através de um campo coberto de mato, e sua passagem deixa um rastro tosco de grama pisada para trás. Por uma questão de conveniência, a próxima pessoa que cruza o campo usa o caminho áspero, que fica mais claramente estabelecido como resultado. Cada pessoa que cruza posteriormente contribui para tornar o caminho mais visível e mais fácil de percorrer. Ninguém constrói o caminho intencionalmente ou como um serviço a outras pessoas; é simplesmente do interesse de cada pessoa usar a rota mais fácil através do campo. No

entanto, o reforço auto interessado do caminho beneficia a todos os que percorrem o campo depois.

Uma das primeiras obras de Mises, *Nation, State and Economy* (1919) analisa o quanto fenômenos sociais mais complexos – como a linguagem – também foram consequências não intencionais de interações individuais. Nenhum comitê ou autoridade central decidiu inventar a fala humana ou publicar um dicionário, muito menos projetar uma linguagem específica como o inglês. De maneira completamente alheia ao benefício da lei, os indivíduos começaram a se comunicar para obter o que queriam uns dos outros. Os sons emitidos gradualmente se tornaram mais redefinidos e variados, mesmo quando os significados de sons específicos se tornaram mais amplamente reconhecidos. A linguagem evoluiu.

Hayek desenvolve um sistema similarmente sofisticado de teoria social para explicar como todas as instituições da sociedade evoluem naturalmente de baixo para cima – das interações voluntárias e não planejadas dos indivíduos – e não de cima para baixo – de especialistas ou poderosos que impuseram sua vontade. As instituições naturais, sustenta Hayek, são os resultados coletivos, mas não intencionais, da interação humana: "é resultado da ação humana, e não da projeção humana". Mesmo fenômenos sociais complexos – como a escrita, a religião ou o dinheiro – são consequências não intencionais da interação humana. A suposta eficiência dos programas governamentais empalideceu em comparação, para dizer o mínimo.

Os construtivistas contra-argumentam que uma sociedade não planejada é caótica e esbanjadora. Com conhecimento suficiente e uma abordagem científica, eles acreditavam que uma sociedade perfeitamente eficiente poderia ser projetada. Sem excedentes, sem escassez, sem desperdício, sem desemprego. Os mercados de ações não entrariam em colapso e as moedas não flutuariam, exceto quando deveriam fazê-lo. A sociedade poderia ser construída de modo que seus membros caminhassem em uníssono em direção aos mesmos objetivos sociais supostamente desejáveis, assim como haviam marchado em uníssono como soldados rumo à vitória na guerra.

A resposta de Mises aos construtivistas reformularia o conceito de individualismo.

O Novo Individualismo Austríaco

Uma nova concepção de individualismo surgiu em resposta a uma teoria que acompanhava o construtivismo. O holismo social tornou-se popular no início do século XX. O holismo social afirma que os sistemas devem ser vistos como totalidades e não como coleções de suas partes, e a dinâmica de um todo difere da soma de suas partes. Em suma, o coletivo é maior e diferente das unidades que o compõem. Uma análise holística da sociedade geralmente começa com um estudo do coletivo, e não do indivíduo, e assume que o comportamento do indivíduo é determinado pelo coletivo. O comportamento individual é definido pelas categorias e propriedades da classe que compõem seu contexto. A sociedade é mais do que a soma total dos indivíduos que a constituem.

Economistas austríacos afirmam o contrário. A sociedade resulta de e é explicada pelo comportamento dos indivíduos que, coletivamente, *são* a sociedade. A sociedade não tem existência independente de seus membros individuais, todos os quais agem em seu próprio interesse. No entanto, o interesse próprio não é equivalente ao egoísmo, pois os atos tradicionalmente altruístas – doar para a caridade, ajudar o próximo, sacrificar-se pela família – são frequentemente vistos pelos indivíduos como um comportamento que enriquece a vida. No que parece um paradoxo para alguns, atos tradicionalmente altruístas são muitas vezes realizados como uma questão de interesse próprio.

Os marxistas acusam aqueles que reduzem a sociedade a indivíduos de serem atomistas; isto é, diz-se que eles fragmentam a sociedade em unidades desconexas e isoladas, de modo que a sociedade não existe verdadeiramente. Em resposta, alguns marxistas chegam ao ponto de afirmar que é o indivíduo, e não a sociedade, que é a verdadeira abstração. Ou seja: os indivíduos não existem sem uma sociedade envolvente, que os defina e os construa. Mises fez uma observação sobre essa posição: “A noção de um indivíduo, dizem os críticos, é uma abstração vazia. O homem real é necessariamente sempre um membro de um todo social”.

Karl Marx argumenta um ponto semelhante a este usando um cenário de Robinson Crusoé, que é uma maneira popular de construir um argumento sobre a natureza humana a partir de seus fundamentos absolutos: o homem isolado. Um indivíduo que nasce e é abandonado em uma ilha deserta, afirma Marx, será mais um ser humano em potencial

do que um ser humano real. (Alguns socialistas, como Hegel, argumentam que o próprio homem era uma abstração.) Marx faz uma distinção entre a "natureza humana em geral" e "natureza humana modificada" por períodos históricos de épocas. Existem dois tipos de impulsos humanos: aqueles que são fixados, como a fome, e aqueles que "devem sua origem a certas estruturas sociais e a certas condições de produção e comunicação". O ponto de Marx é que, além de características inerentes ao instinto, a natureza humana é uma construção social definida pelo contexto social; a sociedade cria a essência humana de seus membros individuais. Isso significa que a sociedade poderia construir o que Marx considera ser o tipo certo de humanidade – como o novo homem soviético – caso as instituições da sociedade fossem totalmente orientadas para alcançar esse objetivo.

Os liberais clássicos argumentam o contrário: uma pessoa criada isoladamente ainda será um ser humano realizado com características humanas que vão muito além de um impulso para as necessidades básicas de sobrevivência. Por exemplo: Crusoé terá uma escala de preferências que os economistas chamam de utilidade marginal decrescente, e ele agirá para atingir primeiro a mais alta; ele obterá água para beber antes de se banhar. Ele terá curiosidade e capacidade de sentir tristeza. Sem interação social, grandes partes de seu potencial nunca se desenvolverão, é claro, mas isso não o torna menos humano ou vazio de vontade e personalidade individuais. Os coletivos oferecem incentivos para comportamentos específicos, mas não definem a humanidade dos indivíduos. São os seres humanos e sua natureza inata que definem o coletivo. Sob a análise de Mises, esse argumento simples evolui para uma nova e abrangente abordagem do individualismo.

Como uma teoria social geral, o individualismo significa a defesa da liberdade individual em oposição ao poder de um coletivo, especialmente o estado. Como uma questão pessoal, significa que as pessoas fazem suas próprias escolhas pacíficas e assumem a responsabilidade por elas. Embora um individualista às vezes seja caracterizado como solitário, o oposto geralmente é verdadeiro, porque os seres humanos são animais sociais – eles anseiam por interação quase tanto quanto por comida e abrigo. A cooperação e o comércio são a realização do individualismo, porque permitem que o indivíduo expresse preferências e satisfaça necessidades. "Uma vez percebido que a divisão do trabalho é a

essência da sociedade", observa Mises, "nada resta da antítese entre indivíduo e sociedade. A contradição entre o princípio individual e o princípio social desaparece".

Um conceito central da filosofia individualista de Mises é a "praxeologia" – uma palavra [práxis] que significa "obra" ou "ação", e que deriva do grego antigo. Seu significado moderno é "o estudo da ação humana, baseado na crença de que o comportamento humano é proposital em oposição a não intencional ou reflexivo, como piscar". Exceto pelo comportamento reflexivo, as pessoas agem, e o fazem porque é de seu interesse fazê-lo, mesmo que seja apenas para remover aquilo que Mises chama de "sensação de insatisfação". Isso acontece tanto para mudar de cadeira, visando aliviar um músculo dolorido, quanto para investir no mercado de ações para garantir a aposentadoria. Toda ação humana é individual, intencional e auto interessada.
Mises então esboça a teoria mais associada a ele. Sua obra-prima *Human Action* descreve o individualismo metodológico:

> "Primeiro devemos perceber que todas as ações são realizadas por indivíduos. Se examinarmos o significado das várias ações realizadas por indivíduos, devemos necessariamente aprender tudo sobre as ações do todo coletivo. Um coletivo social não tem existência ou realidade fora das ações dos membros individuais. Por exemplo: os indivíduos que compunham uma família interagiam uns com os outros dentro de um contexto específico; a soma dessas interações individuais era o que constituía a abstração 'família'."

Mises usa a ideia não ideológica e neutra do individualismo metodológico para descrever a natureza básica da ação humana, bem como para desconstruir a abstração do estado. Se apenas os indivíduos agem, então tudo o que o estado faz ou é pode ser reduzido a ações tomadas pelos indivíduos que coletivamente constituem o estado. Em um exemplo famoso, Mises explica: "É o carrasco, e não o estado, que executa o criminoso. É o significado dessa ação que simboliza, na ação do carrasco, uma ação do estado". Indivíduos que olham para o carrasco veem o estado, mas apenas porque aceitaram a abstração chamada "o estado" como uma estrutura de compreensão do comportamento do carrasco. Sem o contexto do estado, o carrasco seria visto como um assassino, e não como um instrumento de justiça.

Mises admite prontamente que o carrasco age em relação a outros indivíduos, como os juízes, que também constituem o estado; o carrasco faz parte do sistema penal. Ele também pode agir sob coerção, porque a recusa em executar um criminoso pode causar demissão e dificuldades para sua família. Mas a praxeologia está preocupada apenas com o comportamento de um indivíduo, que é o ponto de partida e a única prova observável da preferência individual. A praxeologia não trata das influências sociais ou psicológicas sobre a ação humana; esse trabalho pertence a “outro departamento”. Mises simplesmente afirma que todas as ações são iniciadas e realizadas por indivíduos que agem para promover seus próprios interesses. Explicado de outra forma: não é o estado, mas o carrasco individual que levanta o machado mortal. É o braço do carrasco, e ele não pode escapar da responsabilidade pelas ações que escolhe tomar. (Claro, isso não exonera outros indivíduos envolvidos, como os juízes, por exemplo).

Se apenas os indivíduos agem, então o comportamento coletivo nada mais é do que a soma total das ações e interações dos membros individuais. É comum falar de coletivos ou abstrações como se fossem entidades separadas, que são mais importantes que seus membros. É comum falar dos indivíduos como se agissem e pensassem como um grupo. Quando um homem é preso, por exemplo, o noticiário informa que ele foi apanhado pela polícia. Na realidade, o homem foi algemado por um único policial, e só depois de um único juiz ter assinado o mandado de prisão. Quando ocorre uma batalha, o jornal relata um avanço militar, quando na verdade foram aqueles soldados específicos os únicos a terem de fato avançado. Grupos não agem ou pensam; os indivíduos o fazem; e, às vezes, os indivíduos optam por obedecer a uma autoridade central, que acaba dando a impressão de pensamento coletivo.

O individualismo metodológico soa antissocial para alguns. A impressão também pode ser reforçada pelo uso que Mises faz do exemplo de Robinson Crusoé – o homem isolado – para explicar a praxeologia. No entanto, este uso não sugere que os seres humanos sejam antissociais. Muito pelo contrário. O experimento mental de Crusoé destina-se apenas a remover o fator complicador das relações interpessoais enquanto busca a questão “o que é a ação humana qua ação humana?” É semelhante a um cientista voltando aos princípios fundamentais para entender uma dinâmica. As conclusões de Crusoé são então aplicadas ao mundo real da sociedade.

O *Human Action* explica:

> Se a praxeologia fala do indivíduo solitário, agindo apenas em seu próprio nome e independente dos outros, o faz em prol de uma melhor compreensão dos problemas da cooperação social. Não afirmamos que tais seres humanos autárquicos isolados já tenham vivido, e nem que o estágio social dos ancestrais não humanos do homem, assim como o surgimento dos laços sociais primitivos, tenham se efetivado no mesmo processo. O homem apareceu na cena dos acontecimentos terrenos como um ser social. O homem a-social, isolado, é um constructo fictício. (Nota: Autarquia é a característica da autossuficiência).

A sociedade aumenta o individualismo porque afasta o ser humano do nível animal, permitindo que cada pessoa alcance seu potencial e realize objetivos que seriam impossíveis se buscados de maneira isolada. A interação também é um mecanismo de sobrevivência. A riqueza produzida em conjunto pode ser muito mais abundante do que a riqueza produzida de forma privada, por exemplo, o que deixa todos os envolvidos mais ricos e mais propensos a prosperar. É justamente esse tipo de cooperação que levou a humanidade a dominar o planeta. Os seres humanos são profundamente sociais e as recompensas da sociedade são imensas.

Mises argumenta que os coletivos – como a família ou a sociedade – são abstrações de valor inestimável, pois permitem que as pessoas entendam e descrevam suas interações com outros indivíduos. Os coletivos fornecem o contexto específico para dar sentido à ação individual e à mudança da dinâmica do grupo. Ele explica: "O individualismo metodológico, longe de contestar o significado de tais totalidades coletivas, considera como uma de suas principais tarefas descrever e analisar as origens e as ruínas dessas totalidades, assim como suas estruturas cambiantes e seu funcionamento. E ele o escolhe como o único método adequado para resolver satisfatoriamente esse problema". O individualismo é a chave para entender os coletivos. É a descentralização aplicada à vida real e cotidiana.

E, ainda assim, se apenas os indivíduos agem, como podem surgir instituições coletivas? A resposta volta ao conceito de ordem espontânea desenvolvida por Hayek e outros.

Ordem Espontânea na Produção Econômica

A análise até agora se concentrou em como as instituições e a sociedade *podem* surgir – arguivelmente, como um sistema saudável deve surgir – em função do livre mercado e da livre associação. A dinâmica é bem fácil de ser descrita se usada como referência uma tribo isolada. Mas será que a estrutura do individualismo pode ser expandida do nível local ao global, a fim de fornecer mecanismos complexos, como o comércio internacional, onde os indivíduos geralmente não se conhecem nem interagem diretamente?

No nível local, a cooperação geralmente é intencional. Os agricultores vendem os produtos para os mercados locais; uma equipe de programadores projeta o melhor e mais recente aplicativo; um hospital coordena os horários dos funcionários, com médicos consultando os pacientes; caminhoneiros entregam mercadorias em determinado endereço; um negócio de startup contrata um especialista em marketing. Estes são contatos intencionais e diretos dentro do contexto limitado de uma sociedade.

Como podem indivíduos, de países estrangeiros, que não se conhecem e nem falam a mesma língua, esperar cooperar na criação de alguma coisa? Por acaso não é necessária uma autoridade suprema para a coordenação de estranhos no comércio global? Se assim for, então a autoridade suprema – isto é, o estado – também é necessária internamente, porque todas as nações modernas vivem ou morrem no comércio global. A exigência de centralização reintroduz o estado como um poderoso e legítimo policial da economia.

Mas o comércio global não requer supervisão. Pode parecer paradoxal dizer que estranhos irão cooperar inconscientemente para benefício mútuo porque é do seu próprio interesse fazê-lo. Mas é isso o que acontece. A cooperação não visa a criação de sociedades ou instituições. Cada participante visa enriquecer-se.

"Eu, o Lápis" é um breve ensaio de Leonard Read, fundador da Foundation for Economic Education. É uma curta história contada a partir da perspectiva de um lápis, que narra sua própria criação. A saga começa com a colheita, mineração e formação de matérias-primas em terras distantes, incluindo cedro, cola, cera, grafite, laca e pedra-pomes. Os trabalhadores estrangeiros vendem quantidades definidas para uma variedade de negócios estrangeiros, e o fazem visando ganhar dinheiro

para alimentar suas famílias. Podem desconhecer o destino ou finalidade das matérias-primas; eles podem não se importar, mas eles o fazem mesmo assim.

As tripulações de navios estrangeiros transportam os materiais para um destino específico, onde os estivadores descarregam os contêineres e os caminhoneiros os transportam para uma fábrica de lápis. Os indivíduos da tripulação e os do cais provavelmente são indiferentes ou ignoram o conteúdo da carga, porque recebem os mesmos salários independentemente da remessa. Até este ponto, todos os envolvidos na fabricação de pré-lápis não se importam com os próprios lápis; eles nem mesmo sabem o papel que desempenham no processo da fabricação dos lápis. Seu propósito é, pura e simplesmente, ganhar a vida.

A matéria-prima chega a uma fábrica de lápis, onde pode começar a cooperação autoconsciente para a criação do lápis. Embora as fábricas de lápis hoje sejam provavelmente automatizadas, isso não diminui a cooperação humana necessária para produzir um lápis. Mesmo as fábricas automatizadas exigem supervisão administrativa, assim como fornecedores de equipamentos, reparadores, zeladores, investidores e uma série de outros indivíduos para produzir um único lápis. No entanto, isso não significa que essas pessoas se conheçam, nem necessariamente que se importem com lápis. O que isso tudo de fato significa é que eles querem lucrar com salários e retornos.

O produto de uma multidão de estranhos que agem apenas segundo seus próprios interesses isolados é um lápis.

Em sua introdução a “Eu, o Lápis”, o economista ganhador do Nobel Milton Friedman escreve:

> Nenhuma das milhares de pessoas envolvidas na produção do lápis executou sua tarefa porque queria um lápis. Alguns deles nunca viram um lápis e não sabem para que serve. Cada um vê seu trabalho como uma forma de obter os bens e serviços que deseja: bens e serviços que produzimos para obter o lápis que desejamos. Cada vez que vamos à loja e compramos um lápis, estamos trocando um pouco de nossos serviços pela quantidade infinitesimal de serviços; os serviços que cada um dos milhares de indivíduos prestaram para conseguir o que queriam, e que acabaram por produzir o lápis.

> É ainda mais surpreendente que o lápis tenha sido produzido. Ninguém sentado em um escritório central deu ordens a essas milhares de pessoas. Nenhum policial militar fez cumprir as ordens que não foram obedecidas. Essas pessoas vivem em países diferentes, falam línguas diferentes, praticam religiões diferentes e podem até se odiar – e ainda assim, nenhuma dessas diferenças os impediu de cooperar para, sabendo ou não, produzir um lápis. Mas como foi que isso pôde acontecer? Adam Smith nos deu a resposta […] há duzentos anos.

A resposta de Smith foi a "mão invisível". O termo é introduzido no livro que Smith considera sua obra-prima: A Teoria dos Sentimentos Morais, e reaparece em sua obra subsequente, A Riqueza das Nações. A Mão Invisível refere-se aos benefícios não intencionais, mas imensos para a sociedade, que fluem de pessoas que agem em seus próprios interesses, especialmente no interesse econômico, da maneira descrita pelo conto "Eu, o Lápis". Quase que invisivelmente, a ordem surge das ações auto interessadas de indivíduos, que cooperam com outros de maneira intencional ou não, consciente ou não. A ordem natural declina quando a interação voluntária é prejudicada pela interferência do estado. Em suma, a liberdade traz civilização e prosperidade; o poder produz conflito e pobreza.

"Eu, o Lápis" e "A Mão Invisível" esclarecem outra confusão que pode advir de discussões de ordem espontânea; ou seja: a definição de ordem espontânea como o "resultado da ação humana, mas não da projeção humana" é um pouco ambígua. Claramente, há uma ordem planejada dentro da cadeia de atividades necessárias para fazer um lápis. Os trabalhadores que coletam as matérias-primas trabalham para uma empresa que tem, projetado, um objetivo específico, e o mesmo vale para os trabalhadores dos navios e das docas. A fábrica é uma máquina altamente projetada.

A frase "o resultado da ação humana, mas não da projeção humana" não nega que a produção requer projeção. "Não da projeção humana" significa que nenhum planejador central organiza e coordena qualquer etapa da produção. Toda a organização e estrutura são fornecidas por aqueles indivíduos que, em diferentes etapas, projetam, gerenciam ou trabalham de maneira independente, dentro de suas próprias etapas, para os empreendimentos que resultam, na soma total dessas

etapas, em um lápis. Sem uma autoridade de supervisão, eles se coordenam e funcionam bem. De fato, uma autoridade supervisora seria um obstáculo à sua eficiência. A frase "o resultado da ação humana, mas não da projeção humana" procura explicar como redes complexas podem surgir da cooperação "não intencional": uma cooperação da qual a vida moderna depende.

"Não da projeção humano" refere-se ao exército de estranhos, cujas ações auto interessadas e ostensivamente descentralizadas entregam, sem a necessidade de intenção, uma variedade impressionante de mercadorias. Eles só precisam agir (e sempre agem) em seu próprio interesse. Como resultado, a pessoa média desfruta hoje de um padrão de vida mais alto do que os nobres no passado, incluindo frutas fora de época e uma magnífica variedade de vinhos para acompanhá-las. A cooperação também une as pessoas em paz, porque elas têm interesse em continuar a lucrar umas com as outras por meio do comércio. Multiplique essa cooperação pelos muitos milhões de interações que criam milhões de produtos e serviços, e a dinâmica coletiva se torna uma cola que mantém as sociedades unidas e permite que o comércio global surja: comércio esse que é o motor da paz.

Até agora, a ordem espontânea foi aplicada à economia – a base da sociedade. Dentro da ordem espontânea, a economia é muitas vezes chamada de cataláxia.

A Cripto Como um Fenômeno Econômico Austríaco

> O Bitcoin é melhor entendido quando visto pela lente conceitual da Cataláxia: os participantes do Bitcoin formam espontaneamente um ecossistema monetário e financeiro descentralizado, escolhendo coletivamente o Bitcoin como meio de troca e reserva de valor. O Bitcoin é uma demonstração irrefutável de ordem espontânea na prática.
> – Francis Pouliot

A Cripto-Cataláxia

A teoria praxeológica da cataláxia explica como a ordem *econômica* emerge de um sistema descentralizado, originado das ações descoordenadas e diversas de indivíduos que perseguem seus próprios interesses; é a ordem econômica espontânea. Às vezes chamado de "caláctica", o conceito econômico é um dos avanços intelectuais que permitiram aos defensores do livre mercado explicar como a sociedade evoluiu sem uma autoridade central. Hayek a define como "a ordem trazida pelo ajuste mútuo de muitas economias individuais em um mercado".

O termo obscuro capta a dinâmica que cria a civilização: a cooperação econômica espontânea entre indivíduos e grupos de indivíduos. Se os seres humanos devem se elevar acima do nível de Robinson Crusoé, eles devem interagir em benefício mútuo. A cooperação é tão valiosa para a liberdade individual que Satoshi forneceu o modelo da blockchain gratuitamente como uma forma de melhorar o mundo porque isso melhorou a vida dele. E fez isso segundo seu próprio interesse.

A revolução Satoshi exemplifica como o individualismo metodológico e a cataláxia trabalham juntos. O controle econômico é dado aos indivíduos. As pessoas armazenam suas riquezas em carteiras privadas, com as quais realizam comércio internacional sem passar por um sistema bancário, o que equivaleria a passar pelo estado. A descentralização é reforçada, e não contrariada, pela cooperação de uma rede de pessoas estranhas agindo, cada uma, em seu próprio interesse. E ainda assim, todos os estranhos se beneficiam, mesmo que não gostassem uns

dos outros casos se encontrassem pessoalmente. A criptoeconomia é a verdadeira sociedade econômica.

Ao longo da obra de Hayek, Mises e outros economistas pró-livre mercado, dois conceitos fundamentais emergem repetidamente: individualismo metodológico e ordem espontânea. Os dois conceitos são a espinha dorsal que forma a estrutura ideológica da cripto. Eles também explicam por que a explosão da cripto liberdade foi tão inesperada: surgiu dos indivíduos e da liberdade de ação, que estimulam explosões imprevisíveis de criatividade. Com as criptomoedas, a explosão ocorreu na área mais necessitada: a liberdade financeira.

A área mais difícil de implementar o individualismo metodológico é a financeira, porque ela foi controlada por muito tempo por um dos coletivos mais poderosos que existem: os bancos centrais, que funcionam como braços do estado. Isso significa que as instituições que cercam o banco central foram formadas por sua presença e por suas exigências, e que as atitudes financeiras comuns foram formadas de maneira semelhante.

A sociedade precisa ser lembrada: o estado não produz riqueza. No entanto, o estado precisa de grandes quantias para financiar a burocracia, os militares e outras armadilhas centralizadas do poder. Isso significa que o estado precisa roubar grandes quantidades de riqueza do setor privado – das pessoas comuns. Mas fazê-lo diretamente pode causar resistência na forma de revoltas fiscais ou em algo pior – pior para o estado, é claro. Assim, o estado emite títulos, moeda fiduciária compulsória, incentiva a inflação e compele todo o comércio a passar por instituições corporativistas – compadres dele – que estão sob seu controle. Muitas pessoas aceitam esse status quo como sendo “o jeito que o mundo gira”. Mas o que mais eles sabem? Outros, especialmente aqueles com compreensão da história, sabem que essa situação não é política ou moralmente inevitável, e muito menos necessária. No entanto, por muito tempo os rebeldes encontraram um caminho viável que fosse capaz de contornar a centralização das finanças.

Junte-se à cripto. É uma expressão pura do individualismo metodológico e da ordem espontânea. Mas “É” de que forma? As formas incluem:

- É a descentralização em larga escala. A engenharia central do dinheiro e seu fluxo é incorporada por leis de curso legal, dinheiro

fiduciário inflacionado, bancos centrais, leis de licenciamento financeiro, requisitos de relatórios e outros monopólios econômicos criados artificialmente pelo estado. Enquanto os indivíduos tiverem de seguir as regras do estado, especialmente o uso de fiat e bancos, não haverá liberdade financeira. No que pareceu um instante, mas que na verdade levou anos, Satoshi (e seus predecessores) descentralizou o dinheiro e seus meios de transmissão. As abstrações do estado e dos bancos centrais foram substituídas pelos indivíduos, que agem em seu próprio interesse.

- É descentralização consciente. O objetivo do Bitcoin e da blockchain é contornar a necessidade de uma terceira parte confiável, especificamente o banco central e o estado. A primeira linha de "Bitcoin: A Peer-to-Peer Electronic Cash System" diz: "Uma versão puramente peer-to-peer de dinheiro eletrônico permitiria que pagamentos online fossem enviados diretamente de uma parte para outra sem passar por uma instituição financeira". Ao fazer isso, a criptomoeda ignora as instituições usadas pela elite dominante para roubar riqueza.
- O dinheiro é valorizado pelos indivíduos. Os construtivistas acreditam que o dinheiro é uma construção social, que recebe significado e valor pelo estado da mesma maneira que os seres humanos recebem a humanidade por meio da socialização. Satoshi vira o mundo dos construtivistas de cabeça para baixo. O dinheiro do estado é uma fraude, e ele sabe disso. Os indivíduos que mineram e usam criptomoedas infundem valor nela sempre que a escolhem como meio de troca. E eles não apenas criam riqueza – os indivíduos também definem o valor dela.
- A cripto é profundamente individualista. Isso é verdade não apenas sobre suas funções, mas também sobre sua estrutura. Ela funciona através da involuntária cooperação de indivíduos auto interessados, como por exemplo os "mineradores". A estrutura da blockchain não pode ser centralizada ou nacionalizada; é descentralização exemplificada. Vladimir Putin de forma infame disse que "nem a Rússia, nem qualquer outro país, 'por definição', pode ter sua própria criptomoeda. Se falarmos sobre criptomoedas – isso é algo que vai além das fronteiras nacionais". As criptomoedas em uma blockchain chegam o mais próximo possível de uma

moeda que o estado não pode controlar ou centralizar. Alguns argumentam que as criptomoedas já são coletivistas, porque dependem de uma rede cooperativa de mineradores, nodes, desenvolvedores e administradores; alguns afirmam que a própria rede constitui uma terceira parte confiável. Mas isso não é verdade. A rede é um modelo de como um sistema independente de confiança opera na prática. A acusação confunde cooperação com coletivismo e consenso com planejamento central.

- A cripto expressa o mesmo tipo de ordem espontânea mundial que o conto “Eu, o Lápis.” Em todo o mundo, estranhos involuntariamente cooperam uns com os outros para benefício mútuo. Suas valorações subjetivas e auto interessadas fortalecem algumas criptomoedas e desvalorizam outras, criando e atualizando uma taxa de câmbio para cada uma delas. As criptomoedas prosperaram precisamente porque é um imenso número de estranhos que controlam os nodes, que fazem as transferências, que inovam, que escrevem códigos e, no fim, cooperam. Cada ato é feito por motivos auto interessados, mas que acabam resultando em lucro para si e para os outros.
- A cripto pode parecer caótica, mas expressa uma ordem natural. A ordem centralizada lembra um desfile militar ou as obedientes filas indianas de triagem aeroportuária. A ordem espontânea assemelha-se a uma autoestrada movimentada onde os carros podem mudar de faixa constantemente, entrando e saindo à vontade. O que parece ser caos é uma forma sofisticada de organização, na qual estranhos voluntariamente participam. A autoestrada de aparência caótica leva as pessoas ao seu destino de desejo dia após dia.
- A cripto traz ordem ao campo monetário através de uma diversidade que oferece escolhas quase infinitas. Bancos centrais e instituições financeiras licenciadas pelo estado impõem a uniformidade, porque elas precisam que os clientes estejam em conformidade com os regulamentos e requisitos de relatórios do estado. A uniformidade imposta e a ordem centralizada não refletem as preferências dos indivíduos; eles refletem as preferências do estado. A comunidade cripto evita a uniformidade, porque a cripto atende a indivíduos cujas preferências são incrivelmente diversas. So-

mente quando "uniformidade" é usada como sinônimo de "ordem" que a cripto se torna *des*ordenada. Caso contrário, a cripto espelha o mesmo tipo de ordem que o pregão de uma bolsa de valores.

- O estado é irrelevante e é um obstáculo para a cripto. A centralização requer o estado ou algum substituto equivalente, porque a uniformidade não é natural e, para ser "aceita" deve ser empurrada goela abaixo. A descentralização, por sua vez, não requer um estado, porque não há conformidade forçada de ação ou preferência. Todas as escolhas são feitas livremente pelos indivíduos envolvidos.
- A cripto é a "mão invisível" da moeda. O termo descreve os benefícios sociais e econômicos não intencionais de ações tomadas pelos indivíduos visando seus próprios interesses. Ao perseguir seus próprios interesses financeiros, os usuários de cripto fazem muito mais para valorizar a moeda e criar práticas financeiras sólidas do que reformadores, que protestam por mudanças dentro do status quo sem questionar seus fundamentos… e sem conseguir resultados.

A cripto é uma expressão pura da economia austríaca.

Os Aspectos Revolucionários Não Reconhecidos da Cripto

A cripto lembra a "teoria do atirador solitário". Embora o termo seja geralmente associado ao assassinato do presidente John Kennedy e à subsequente Warren Commission, seu significado pode ser expandido. A história tropeça ao longo de um caminho bastante estável, embora nem sempre fácil, que é amplamente planejado pelo estado. Então um atirador solitário salta dos arbustos e atira no arquiduque Francisco Ferdinando, da Áustria, no Presidente McKinley, ou em JFK. A sociedade vira de cabeça para baixo. No caso de Ferdinando, o assassinato desencadeou a Primeira Guerra Mundial. A história muda para sempre, e a mudança não pode ser desfeita.

O controle estatal do mundo financeiro avançou esplendidamente ao longo do século XX – ou miseravelmente, dependendo da sua perspectiva. Uma rede mundial de controle foi lançada sobre as finanças dos indivíduos através de medidas como a Foreign Account Tax Com-

pliance Act (FATCA), que tentou garantir que os indivíduos que buscavam a liberdade não tivessem para onde ir com seu dinheiro. Então a cripto salta dos arbustos e assassina o sistema bancário. A história econômica muda para sempre, e a mudança não pode ser desfeita.

O efeito da cripto nas instituições financeiras estatais é bem conhecido, mas os efeitos sobre política social são menos discutidos. Previsivelmente, a explosão de liberdade que abalou o sistema bancário central também impactou outras instituições e políticas do estado. Aqui estão algumas poucas:

Política estrangeira. A comida é frequentemente usada como arma de política externa. Um artigo do *Free Thought Project* descreve como a blockchain neutraliza o uso belicoso de alimentos: "A tecnologia revolucionária da blockchain está ajudando a vítimas de desastres & alimentando os famintos sem estado". "Enquanto estados e banqueiros afirmam que criptomoedas e blockchain são ferramentas de criminosos, milhões de dólares em ajuda – gerados por essas tecnologias – estão ajudando os menos afortunados em todo o mundo". A ideia central do artigo é que as criptomoedas permitem que nações e indivíduos carentes contornem sanções econômicas impostas a eles por nações mais poderosas. Tornou-se mais difícil deixar as pessoas famintas por vantagens políticas.

Política doméstica. Quando o estado da Venezuela desvalorizou o Bolívar, removendo três zeros da moeda, os cidadãos migraram para a alternativa de livre mercado do bitcoin, com a qual eles já estavam familiarizados. "Nas economias avançadas, criptomoedas ativas como o bitcoin até agora tiveram pouco propósito além de especulação e jogos de azar. Mas nos países onde o sistema monetário e as estruturas financeiras estão desmoronando, o bitcoin pôde fornecer uma reserva alternativa de valor em relação à já demasiadamente inflacionada moeda local". A cripto resgata empresas; ela salva vidas.

O Controle Social do "Vício". A "Operação Chokepoint" foi uma operação bancária e política da era Obama, que atacava negócios supostamente indesejáveis, mas legais, como a venda de maconha medicinal, sexo e armas. O sistema bancário fechou contas, cancelou cartões de crédito e negou todos os seus serviços aos clientes "malfeitores". Essa prática está sendo revivida hoje. Mais uma vez, os bancos estão mirando nas lojas de maconha, nos profissionais do sexo e nas empresas de armas, independentemente de eles estarem ou não realizando um ne-

gócio legal. Cada vez mais, os vendedores de bens e serviços desaprovados têm adotado as criptomoedas como forma de sustentar seus meios de subsistência.

Proteção da Liberdade de Expressão. Depois de fazer circular documentos que constrangiam estados, o Wikileaks enfrentou um bloqueio bancário que acabou com as doações, que eram seu sangue vital. Então a Wikileaks abriu doações via bitcoin e a riqueza foi mais uma vez derramada sobre a empresa. A censura foi evitada. O mesmo acontece com a indústria pornográfica, que é um alvo da Operação Chokepoint.

O Livre Fluxo de Informações. Os processos contra a propriedade intelectual são geralmente baseados em seguir a trilha do dinheiro e descobrir os indivíduos do outro lado. Mas com o anonimato criptográfico, essa estratégia cai por água abaixo. Um artigo do site bitcoin.com, intitulado “Escritório de Propriedade Intelectual [IP] da UE: Bitcoin impede esforços antipirataria”, explica: “A ameaça inerente ao Bitcoin, de acordo com o relatório, é que as transações não podem ser facilmente vinculadas a um indivíduo no mundo real. Este problema é ruim para o EUIPO, uma vez que a aplicação dos direitos de autor é normalmente baseada na estratégia de seguir a trilha do dinheiro”. Isso beneficia o fluxo global de informações.

Política de imigração. A imigração e a migração temporária são muitas vezes motivadas por um desejo de enviar dinheiro de volta para casa. Mas os migrantes também são frequentemente “desbancarizados” por instituições financeiras que exigem documentação, e a única alternativa é pagar taxas enormes para enviar dinheiro através de uma empresa privada, com suas famílias esperando dias pelas transferências. O presidente Trump ameaçou cortar esse incentivo à migração ao fechar ainda mais canais de transmissão. Mas, infelizmente, transferências rápidas e baratas via criptomoedas são incrivelmente difíceis de controlar.

O Estrangulamento dos Advogados e dos Tribunais. Contratos inteligentes são contratos jurídicos vinculados que usam software para auto executar os termos do contrato. Os contratos inteligentes peer-to-peer podem um dia se tornar onipresentes, desde negócios imobiliários até pedidos de seguro, o que reduzirá drasticamente a necessidade de advogados.

A Autonomia da Família. Os impostos sobre herança são hediondos porque são uma dupla tributação: assim que morre e passa suas pro-

priedades remanescentes para sua família, a pessoa cuja riqueza foi tributada por toda a vida é cobrada mais uma vez pelo estado. A cripto divide invisivelmente os bens entre os entes queridos – não há espaço para o estado na família.

Tudo isso é apenas uma pequena amostra do impacto revolucionário do uso das criptomoedas. As instituições que servem ao livre mercado estão sendo lentamente devolvidas ao controle e serviço dos indivíduos. As instituições que atendem ao estado estão sendo ignoradas e afundando cada vez mais.

As criptomoedas são o dinheiro da sociedade, não do estado. Sua evolução oferece um raro vislumbre de como instituições essenciais podem surgir em um livre mercado, sem a assistência do estado. A cripto de livre mercado é a manifestação do individualismo metodológico e da ordem espontânea em grande escala em uma área essencial da vida: a privacidade financeira.

Descentralização como Desobediência

A descentralização como estratégia para a liberdade acontece quando indivíduos buscam empoderar-se, separando-se do estado e reivindicando sua autonomia como indivíduos. Uma maneira de se separar é desobedecer à lei. A maioria das pessoas desobedece a lei de maneiras triviais e pacíficas todos os dias de suas vidas. Elas ignoram os limites de velocidade, constroem um anexo não autorizado à sua casa, cruzam o sinal vermelho, mentem nos formulários do estado, recebem pagamentos por baixo da mesa, queimam lixo no quintal, andam no meio da rua, recusam perguntas do censo, passeiam com o cachorro sem coleira ou sem licença e enviam mensagens de texto enquanto dirigem. Essas pequenas ofensas trazem pouco risco além de uma multa, mas mostram que as pessoas não se importam com a desobediência a leis que não fazem sentido ou que as incomodam de forma irracional.

Depois, há aqueles que desobedecem a lei de maneira mais séria. Eles sonegam impostos, estabelecem negócios não licenciados, usam drogas ilegais, mentem para a polícia, trocam sexo por dinheiro ou contrabandeiam. Esses delitos acarretam uma possível pena de prisão, mas a disposição das pessoas em desobedecer mostra que uma parcela significativa da população despreza as leis de crimes sem vítimas com tanto desprezo que elas as não cumprem, mesmo com risco considerável para seu bem-estar.

Nos anos 80, uma estratégia popular pela qual os indivíduos descentralizavam completamente suas vidas ficou conhecida como "Browning-out", porque os praticantes usavam o livro best-seller de Harry Browne, *How I Found Freedom in an Unfree World: A Handbook for Personal Freedom,* como um modelo. Browne define a liberdade como viver a vida como você deseja viver enquanto permite que outros façam o mesmo. Em vez de protestar contra o estado ou buscar reformas distantes por meio de organizações, como os republicanos ou os democratas, Browne afirma que as pessoas podem desfrutar de um alto grau de liberdade aqui e agora. O capítulo 7 de seu livro, intitulado "As Armadilhas do estado", afirma: "Mas quem é a 'sociedade', senão as pessoas que já expressam suas necessidades e preferências no mercado? Se elas não estão dispostas a pagar pelo serviço no livre mercado, quem pode dizer que estão dispostos a pagar por ele através do estado? Todas as ações do estado dependem de transações unilaterais, nas quais um indivíduo é forçado a escolher entre pagar pelo que não quer ou ir para a cadeia". Aqueles que Browned-out (saíram como Browne) da Armadilha do estado descentralizaram o poder em suas vidas para o nível pessoal, onde eles eram a única autoridade sobre suas próprias escolhas.

Sair da sociedade tem um custo alto, no entanto. Não é apenas que o Estado tenta dar exemplos de dissidentes. É também que a sociedade é um benefício incrível para a humanidade. Facilita "bens" como conhecimento, prosperidade, cultura, progresso e autorrealização emocional de uma maneira impossível para os seres humanos isolados. Retirar-se torna-se preferível apenas quando uma sociedade é tão totalitária que constitui um perigo ou tormento para a própria vida. Esse é o ponto ao qual os escravos americanos arriscaram suas vidas para fugir do Norte, com cães e homens armados em seus calcanhares. Esse é o ponto ao qual pessoas desesperadas escalaram um muro de arame farpado em Berlim Oriental, apesar das armas apontadas em suas costas. Pessoas desesperadas tentaram escapar de uma selvageria que se faz passar por ordem social, e arriscaram suas vidas para fazê-lo.

A lição: a sociedade só tem valor para os indivíduos na medida em que eles têm a capacidade de dizer "não". Nada é um "bem" incondicional; até mesmo o alimento com o qual a vida se sustenta não é um bem incondicional. Pergunte às pessoas que desejam cometer suicídio ou a um prisioneiro em greve de fome. O que é bom ou ruim depende de circunstâncias que devem ser avaliadas pelo próprio indivíduo. O

valor da sociedade depende da descentralização do poder, porque só assim os indivíduos que a compõem poderão sempre dizer "não".

A cripto fornece uma nova estratégia de liberdade, que evita muitas das desvantagens da desobediência aberta ou emigração; ela oferece uma revolução pacífica baseada no interesse próprio e que contorna o estado, em vez de enfrentá-lo. As pessoas podem dizer "não" a aspectos intoleráveis da sociedade, como o monopólio monetário, enquanto permanecem fisicamente conectadas com o resto.

Para muitos, uma revolução pacífica soa como uma contradição em termos. A confusão envolve a questão da revolução, porque ela foi mal retratada na ciência política e mal representada na realidade. Ruas com barricadas, pessoas em fúria, carros em chamas, confrontos com militares, gás lacrimogêneo, vitrines quebradas de lojas saqueadas... isso não é revolução. A verdadeira mudança vem dos corações e mentes das pessoas quando elas abraçam uma nova ideia, uma nova visão. A verdadeira revolução não é raiva e desespero; é esperança e realização.

John Adams escreveu a Thomas Jefferson sobre a Revolução Americana. "O que queremos dizer com Revolução? Guerra? Isso não fazia parte da Revolução. Foi apenas um Efeito e Consequência disso. A Revolução estava na mente do povo, e isso foi efetuado, de 1760 a 1775, no decorrer de quinze anos antes que uma única gota de sangue sequer fosse derramada em Lexington." Adams explicou onde a Revolução Americana poderia ser encontrada. "Os registros de treze legislaturas [coloniais], os panfletos, jornais em todas as colônias devem ser consultados, durante esse período". Durante quinze anos antes do levante, oradores e escritores vinham educando incessantemente o público sobre seus direitos naturais e a common law (lei comum). Essa foi a verdadeira Revolução Americana.

Uma revolução social nada mais é do que uma mudança fundamental em uma sociedade que transfere o poder de um grupo ou classe para outro. A verdadeira revolução ocorre somente depois que as bases intelectuais foram estabelecidas para mudar os corações e mentes de uma parcela suficientemente significativa da população; alguns estimam que a porção não deve ser superior a 10%. Se as bases intelectuais não foram estabelecidas, então as erupções violentas inevitavelmente se transformam em golpes, com um novo grupo de elites substituindo o antigo grupo. Enquanto for politicamente liderada, a revolução retornará ao "novo chefe, igual ao antigo chefe", e os indivíduos não serão empoderados.

Uma revolução de e para as pessoas comuns significa que a mudança no poder é descentralizada das elites para o nível individual. A violência apenas interfere nesse processo. É tentador especular o que teria acontecido se a revolução intelectual nas colônias americanas não tivesse sido interrompida pela violência. A verdadeira revolução referenciada por Adams estava lentamente conquistando a lealdade das pessoas comuns, e poderia ter produzido uma derrubada não violenta do jugo britânico. Como seria a América agora se não tivesse nascido com sangue? Felizmente, seu verdadeiro nascimento foi no papel de jornal, o que pode explicar por que terminou melhor do que a Revolução Francesa.

A explosão silenciosa causada por Satoshi em 2008 foi "uma revolução" porque derrubou a realidade do controle financeiro estatal e descentralizou o poder do estado para a pessoa comum. Aqueles que chamam o Bitcoin de revolucionário, no entanto, são descartados como hiperbólicos, porque a erupção criptográfica não está de acordo com as imagens de ruas ocupadas com barricadas e pessoas gritando "estado de merda!". Os pioneiros das criptomoedas não se assemelham a revolucionários armados, atirando na selva aos moldes de Che Guevara. O próprio Satoshi permanece anônimo, e isso é inédito para um líder revolucionário. E o Bitcoin rompe com esse estereótipo de revolução de várias maneiras. Foi uma revolução modesta e despretensiosa, em que nenhum sangue foi derramado. A área da vida que causou turbulência foi a finança – também conhecida como "lucro imundo" – e *isso* raramente é considerado uma causa nobre, digna de uma revolução. Não deveria uma bandeira que se preze dizer "LIBERDADE, JUSTIÇA" em vez de "DINHEIRO PRIVADO"?

Isso acontece porque a independência financeira é liberdade e justiça. A capacidade das pessoas de fazer e manter a riqueza que ganham é a maneira como elas alimentam seus filhos e perseguem sonhos; é como elas passam da fome ao bem-estar; a riqueza permite que as pessoas possuam a terra em que andam; o "lucro imundo" transforma uma assembleia de estranhos em uma sociedade civil, em indivíduos que negociam uns com os outros em vez de fazerem guerra uns contra os outros. O dinheiro é o motor da própria civilização porque a liberdade de expressão, a arte, a literatura e as outras incríveis conquistas humanas só acontecem quando as pessoas conseguem se alimentar.

A Revolução Satoshi é uma revolução das esperanças crescentes, que se tornou possível através da descentralização do controle econômico que as criptomoedas forjaram. É uma revolução de pessoas comuns, que agora têm uma alternativa viável ao fiat opressivo e aos bancos centrais.

"A revolução das esperanças crescentes" refere-se a uma situação em que mesmo um leve aumento na prosperidade e na liberdade leva as pessoas comuns a acreditar que podem melhorar suas vidas por meio de seus próprios esforços. Essa crença os faz exigirem mudanças políticas e econômicas que tragam mais liberdade e mais prosperidade. A pessoa comum não é uma lutadora da liberdade, e sua demanda por mudança não depende de ideologia. Depende do interesse próprio. Elas querem uma vida melhor para si mesmas e para seus filhos. E para *isso*, estão dispostas a lutar – principalmente de forma não violenta.

A frase "revolução das expectativas crescentes" surgiu depois que a Segunda Guerra Mundial desestabilizou a estrutura de poder do mundo. As ex-colônias do Extremo Oriente à América Latina e África se livraram do imperialismo e do despotismo, porque as pessoas comuns vislumbraram a possibilidade de finalmente alcançar mais liberdade e prosperidade.

O advento das criptomoedas desestabilizou a estrutura de poder financeiro do mundo e está causando uma segunda revolução de esperanças crescentes. Isso não ocorre em nível nacional – a cripto não reconhece fronteiras – mas sim na vida dos indivíduos, que podem finalmente controlar suas próprias finanças em privacidade e independentemente de permissão. Isso tem implicações políticas profundas, é claro, porque as pessoas independentes são muito menos propensas a obedecer.

Toda revolução bem-sucedida deve responder: "Qual é o ponto final?" Se não houver uma boa resposta, então um sistema ruim será substituído por outro sistema ruim, que despencará no vazio. A Revolução Francesa derrubou uma monarquia corrupta apenas para vê-la substituída por um "Comitê de Segurança Pública", que instituiu o que ficou conhecido como "O Reino do Terror". A revolução Satoshi deve responder: "Qual é o ponto final?". Gandhi disse: "os meios são os fins em andamento". Para aqueles que acreditam na cripto, a descentralização é o meio; a descentralização é o fim em andamento: o empoderamento total dos indivíduos.

Anarquismo: o Ponto Final da Descentralização

O homem nasce livre, mas encontra suas correntes em todo canto.
– Jean Jacques Rousseau

Existe tanta confusão e calúnia cercando o termo “anarquismo” que é útil, senão necessário, introduzir o conceito através de uma explicação… Daquilo que ele não é.

- Anarquismo não é violência. A maioria das tradições é explicitamente pacífica. O anarquismo não violento de Henry David Thoreau e de Mahatma Gandhi são exemplos.
- O anarquismo não é caos. Significa “sem estado”, e não “sem ordem”.
- Anarquismo não é pacifismo. Algumas formas, como o anarquismo cristão promovido por Leon Tolstói, mantêm o pacifismo como um princípio central, mas a maioria das tradições reconhece plenamente o direito de usar a força em autodefesa.
- O anarquismo não é inerentemente de esquerda. O anarquismo de esquerda recebeu a maior parte da atenção histórica, mas o primeiro anarquista americano foi o libertário Josiah Warren (1798-1874).
- O anarquismo não é um ideal impraticável. É uma abordagem realista para viver em sociedade sem sacrificar a individualidade.

Se isso tudo é aquilo que o anarquismo não é, então o que é o anarquismo? Simplificando, anarquismo significa “sem o estado”.

Mas o que é o estado? É a instituição que reivindica jurisdição sobre determinado território e o monopólio do uso da força. O estado é uma força institucionalizada, que exige obediência das pessoas que vivem neste território. O anarquismo olha para o estado e não vê serviços pelos quais as pessoas pagam impostos. Aquilo que é dito como serviço é, na realidade, monopólio sustentado pelo roubo e pela força.

Uma das maneiras mais fáceis de entender como o anarquismo funciona é perceber que é assim que a maioria das pessoas conduz suas vidas diárias. Elas vivem sem o estado, e nem se dão conta disso. O

anarquismo é a filosofia que eles seguem com a família, amigos, parceiros de negócios e até estranhos. Quando uma pessoa acorda de manhã, nenhuma lei a obriga a alimentar seus filhos com café da manhã em vez de deixá-los morrer de fome, ou a beijar sua parceira em vez de espancá-la. Quando ela pega carona com colegas para o trabalho, não há nenhum policial presente para impedi-lo de roubar seus bolsos ou socá-los no nariz. Ao longo do dia, nenhum burocrata fica por perto para garantir que ele pague por uma xícara de café ou contribua com sua parte da conta do almoço. Enquanto anda pela rua, um homem não ataca estranhos aleatórios ou puxa uma mulher para o beco a fim de molestá-la. Quando um estranho começa a sair do meio-fio em direção a um veículo que se aproxima numa velocidade considerável, alguém estende a mão rapidamente para impedir a pessoa.

Não é o estado que faz as pessoas agirem com decência habitual. É a sociedade civil, a família e os laços da humanidade que o fazem. A sociedade civil é naturalmente pacífica porque consiste em trocas voluntárias e não coercitivas. É da sociedade civil que os homens adquirem os hábitos e as recompensas da cooperação. Dito de outra forma, a maioria dos indivíduos já lida uns com os outros em suas vidas diárias como se todos vivessem sob a anarquia.

É o estado e outros criminosos que introduzem a força na vida cotidiana. O estado chega na forma da lei monopolizada através da ponta de uma arma. O estado diz a uma pessoa: “você não pode abrir um negócio, porque competiria conosco ou com alguma corporação favorecida por nós”. Diz que “sua propriedade não é sua para usar, mas nossa para administrar, tributar e confiscar se você se recusar a obedecer”. O estado rouba os ganhos de uma pessoa para sustentar seus próprios empreendimentos, até mesmo aqueles que causam repulsa na pessoa, como a guerra; o estado diz: “seu dinheiro é nosso para gastar como *nós* quisermos, e sua consciência não importa”. O estado exige a sua obediência a uma miríade de leis babás que trivializam o suposto direito de escolha individual que ele oferece. O estado tenta determinar até o tipo de canudo que alguém pode usar para beber refrigerante. O estado afirma: “você é meu para comandar.”

Em contraste, os anarquistas dizem às pessoas pacíficas: “abra qualquer negócio que desejar”; “sua propriedade é sua”; “seu dinheiro e sua alma são seus”, e “o estado não tem autoridade sobre você.”

Se o anterior não soa como o anarquismo que geralmente se discute, é porque existem diferentes tradições de anarquismo, e as mais

barulhentas e violentas recebem mais atenção. As várias formas de anarquismo incluem anarquismo individualista, anarquismo comunista, anarquismo socialista, anarquismo mutualista, anarquismo cristão, anarco-sindicalismo e anarcocapitalismo. O que os une? O que os separa?

As tradições dentro do anarquismo concordam que o estado é um tipo de grupo baseado na violência organizada e que é indesejável; é isso que une os anarquismos hifenizados – a rejeição do estado e da violência organizada como um todo. Onde eles discordam, porém, é sobre o que constitui violência e como uma sociedade sem ela funcionaria.

Eis o contraste entre as abordagens dos anarquismos comunistas e individualistas.

O comunismo vê o capitalismo laissez-faire como uma forma de roubo, que é uma forma de violência. Um dos motivos é o "valor excedente" – a famosa mais-valia. Popularizado por Karl Marx, esse conceito refere-se ao valor supostamente criado pelos trabalhadores, que excede os custos de seu trabalho e produção. De forma simplista: Um operário ganha $1 por hora e usa matéria-prima que custa $1 para produzir um bem que é vendido por $10. Segundo Marx, uma mais-valia de $8 foi criada pelo trabalhador, que é o legítimo proprietário dessa quantia. A mais-valia é embolsada pelo dono da fábrica capitalista em um ato de roubo. O capitalista é capaz de roubar os $8 porque possui os meios de produção que são protegidos pela força do estado. Assim, o capitalismo está irrevogavelmente enredado na exploração dos trabalhadores e na violação de seus direitos. Para os esquerdistas, o anarquismo é necessariamente antiestatista e anticapitalista porque ambos são formas de violência.

O anarquismo individualista desafia essa interpretação. Ele olha para o mesmo operário e proprietário da fábrica e vê uma relação consensual pela qual o trabalhador recebe um salário com o qual ambos concordaram e através do qual ambos se beneficiam. A chamada mais-valia ou lucro que o capitalista recebe é em troca dos riscos de fazer negócios, das despesas gerais, do investimento contínuo de capital, dos custos de propaganda e do custo de seu próprio tempo. Nenhuma força ou fraude está presente. Desde que o estado não promova o lucro do capitalista, fazendo nada além de fazer valer os direitos de propriedade – por exemplo, ele não lhe concede um monopólio – então nenhuma força ou fraude está presente devida ao estado. A fábrica expressa apenas o livre mercado e a troca voluntária.

Se o estado intervém, aprovando leis que favorecem ou prejudicam os negócios, então o arranjo deixa de ser de livre mercado ou capitalismo de laissez-faire e se torna capitalismo de compadrio; este é um arranjo no qual o estado e algumas empresas se alinham em benefício mútuo e em desvantagem de todos os outros. Os que mais sofrem são os trabalhadores, as empresas concorrentes e os consumidores. Para os anarquistas individualistas, o anarquismo é antiestado e anti-comparsas-do-estado. O anarquismo individualista é pró-mercado e capitalista.

O profundo desacordo sobre o livre mercado tem implicações para os conceitos-chave usados por ambas as formas de anarquismo. Por exemplo, o anarquismo comunista e o anarquismo individualista definem "classe" e afiliação de classe de maneiras drasticamente diferentes. O anarquismo comunista define a filiação de classe de uma pessoa por referência à sua relação com os meios de produção; alguém é trabalhador ou capitalista; ele é explorado ou explorador. As duas classes estão presas em uma guerra de classes sem fim.

Em contraste, o anarquismo individualista define a filiação de classe com referência à relação de uma pessoa com o poder do estado; ele coopera com os outros de forma voluntária (sociedade) ou usa a força (o estado). Ou ele é um membro produtivo da sociedade ou ele é um criminoso. Os anarquistas individualistas veem as duas classes – a sociedade e o estado – presas em uma guerra de classes insolúvel.

Em resumo: embora todas as formas de anarquismo rejeitem o estado e sua violência organizada, algumas formas de anarquismo discordam profundamente sobre o que constitui violência.

O que é o Anarquismo Individualista ou Libertário?

> Isso nos leva ao Anarquismo, que pode ser descrito como a doutrina de que todos os assuntos dos homens devem ser administrados por indivíduos ou associações voluntárias, e que o estado deve ser abolido. Quando Warren e Proudhon, prosseguindo em sua busca por justiça ao trabalho, se depararam com o obstáculo dos monopólios de classe, viram que esses monopólios repousavam sobre a Autoridade, e concluíram que a coisa a ser feita era não fortalecer essa Autoridade e assim tornar o monopólio universal, erradicar totalmente a Autoridade e dar total domínio ao princípio

oposto, a Liberdade, tornando a competição, a antítese do monopólio, universal.
– Benjamin R. Tucker

Aqueles que chamam a si mesmos de individualistas ou anarquistas-libertários não concordam em todos os aspectos da teoria. Afinal, eles são anarquistas. O que precede, entretanto, é a visão dominante. O anarquismo individualista geralmente se baseia na Lei Natural da qual surgem os direitos naturais ou individuais. A palavra "Lei" aqui não é usada em sentido legal ou legislativo. Refere-se a um princípio ou uma regra governante, como as leis da física. "Natural" significa que a lei é baseada nos fatos da realidade e na natureza do homem.

Em sua forma mais simples, a versão da Lei Natural usada pelo anarquismo individualista é uma tentativa de fundamentar os valores humanos nos fatos da realidade e da natureza humana. Dito de outra forma: Dado o que sabemos sobre a realidade e sobre a natureza humana, é possível raciocinar regras de comportamento que maximizem o bem-estar dos seres humanos? O anarquismo individualista responde "sim!" e se volta para o conceito de direitos naturais ou individuais. Ele pergunta: "quem é o dono do indivíduo?" Como discutido anteriormente, existem apenas três respostas possíveis: é o indivíduo (liberdade pessoal), é alguém ou alguma outra coisa (escravidão), ou ele é propriedade não reclamada. O anarquismo individualista argumenta fortemente a favor da primeira posição.

A reivindicação de uma pessoa sobre seu próprio corpo é descrita com diferentes termos, incluindo "soberania do indivíduo", "donidade de si mesmo", "autonomia", "autopropriedade" e "direitos individuais". Mas para reivindicar seu direito inato de liberdade, todo homem deve respeitar a liberdade igual dos outros. Se ele inicia a força, então suas ações constituem uma declaração de que ele não considera a liberdade como seu direito de nascença ou qualquer direito. Os direitos são universais – existem no mesmo grau dentro de cada ser humano – ou não são baseados na natureza humana. É este dever de respeitar os direitos dos outros que um indivíduo carrega consigo dentro da sociedade.

Direitos e deveres são as ferramentas pelas quais a sociedade resolve conflitos e evita a violência. O individualista do século XIX Benjamin R. Tucker usa essa abordagem enquanto especula sobre a natureza da propriedade. Tucker acredita que as ideias surgiram apenas porque atendem a uma necessidade ou porque respondem a uma pergunta.

Para ilustrar seu ponto de vista, Tucker pede aos leitores que imaginem um universo paralelo ao nosso, mas que siga regras diferentes. Nesse universo paralelo, os habitantes podem satisfazer suas necessidades simplesmente desejando bens. Comida aparece magicamente em suas mãos, roupas milagrosamente cobrem seus membros e uma cama surge sob seus corpos cansados. É pouco provável que essa sociedade paralela venha com o conceito de propriedade privada. Por quê?

Tucker pergunta: “O que há na realidade de nosso próprio mundo e na natureza do homem que dá origem ao conceito de propriedade em primeiro lugar?”. Ele conclui que a ideia de propriedade surge como forma de resolver conflitos causados pela escassez. No universo real, quase todos os bens são escassos, e isso leva à competição pelo seu uso. Como a mesma cadeira não pode ser usada da mesma maneira ao mesmo tempo por duas pessoas, é necessário determinar quem deve usar a cadeira. O conceito de propriedade resolve esse problema social. O proprietário da cadeira deve determinar seu uso. “Se fosse possível”, escreve Tucker, “e se sempre tivesse sido possível, para um número ilimitado de indivíduos usar em uma extensão ilimitada e em um número ilimitado de lugares a mesma coisa concreta ao mesmo tempo, jamais teria sido instituída qualquer coisa como a propriedade.”

Quaisquer direitos, deveres e propriedades são derivados – seja da lei natural ou do utilitarismo. Eles são o contexto que os indivíduos trazem consigo quando entram na sociedade.

Uma Saudação a Henry David Thoreau

Poucos filósofos do século XIX usaram a sua própria capacitação com tanta graça quanto o americano Henry David Thoreau. Ele tinha boas razões para se perguntar: “Como o indivíduo lida com um estado moralmente intrusivo?” Sua solução é simples; jogue o estado fora de sua vida e nunca olhe para trás. Foi isso que Thoreau fez na vida real.

O tratado político mais famoso de Thoreau se chama *Desobediência Civil*. Foi sua resposta a uma prisão durante a noite de 1846 por se recusar a pagar um imposto que violou sua consciência. Uma troca famosa e talvez anedótica ocorreu enquanto ele estava preso. Ralph Waldo Emerson o visitou e cobrou-lhe o pagamento de uma multa para que fosse libertado.

Emerson pergunta: “Henry, o que você está fazendo aí dentro?”

Thoreau responde: “Waldo, a verdadeira questão é: o que você está fazendo aí fora?”

Thoreau não ficou amargurado com sua breve prisão. Perto do fim de sua vida, ele foi perguntado: “Você fez as pazes com Deus?” Ele respondeu: “Nunca briguei com ele”. Para Thoreau, esse teria sido o custo real do pagamento do imposto; significaria brigar com sua própria consciência, o que seria semelhante a brigar com Deus.

A Desobediência Civil termina com uma nota feliz. Após a libertação de Thoreau da prisão, as crianças de sua cidade natal imploraram para que ele se juntasse a uma caçada por mirtilos. Caçar mirtilos era um dos passatempos valiosos de Thoreau, e sua habilidade em localizar arbustos carregados de frutas o tornou o favorito das crianças. Ele termina sua crônica de prisão com as palavras: “Eu me juntei a um grupo de caçadores de mirtilos, que estavam impacientes para se submeterem à minha liderança; e em meia hora estávamos no meio de um campo de mirtilos, em uma de nossas colinas mais altas, a duas milhas de distância, e lá o estado não foi visto em lugar algum.”

E lá o estado não foi visto em lugar algum. Este é o legado de Thoreau e Satoshi para aqueles que desejam compreender isso: para aqueles que estão dispostos a abandoná-lo e não olhar para trás, o estado não será visto em lugar algum. Thoreau, em sua alegria de correr com as crianças, sabia que a prisão não era a sua realidade. Caçar mirtilos era a sua realidade.

O que resta quando não há estado? Indivíduos, sociedade… e mirtilos![1]

1 Nota de Tradução: Um trecho dessa parte específica foi uma adição considerada pertinente pela equipe de tradução. No original lê-se Individuals and Society (indivíduos e sociedade).

S E Ç Ã O   Q U A T R O

Estado e Sociedade

Relevância do Estado, da Sociedade e da Obediência para a Cripto

> O muro que separa o estado e a sociedade está desmoronando. Ou melhor, o estado está martelando em uma tentativa agressiva de controlar todos os aspectos da vida produtiva e cooperativa. […] As pessoas com quem você lida diariamente estão deixando de ser bons vizinhos, comerciantes honestos e estranhos desinteressados. Eles estão se tornando informantes do estado que monitoram sua expressão, seu dinheiro, seu comportamento e atitude para denunciá-lo às autoridades. Eles estão deixando de ser "sociedade" e se tornando "o estado".
> – Murray Rothbard, "Society Without State".

O liberalismo clássico traça uma distinção nítida entre o estado e a sociedade, que as criptos adotam. A cripto não foi projetada para imitar moeda emitida pelo estado ou sistemas monetários controlados pelo estado. Sua estrutura e função foram criadas para empoderar o indivíduo através do fornecimento de meios livres do estado para alcançar a independência financeira. Seus fins e seus meios são tão compatíveis com a sociedade quanto antagônicos ao estado.

Os conceitos e realidades de estado, sociedade e obediência são o contexto no qual o Bitcoin nasceu e no qual as criptomoedas agora operam. Para entender o passado, presente e futuro das criptomoedas, é necessário entender esses conceitos.

A Estrutura do estado, da Sociedade e das criptomoedas

> O problema dos meios é, a meu ver, um problema duplo: primeiro, o problema do fim e dos meios; segundo, o problema do Povo e do estado, ou seja, os meios pelos quais o povo pode supervisionar ou controlar o estado […]. Os meios devem ser proporcionados e adequados ao fim, pois são meios para o fim, por assim dizer, o próprio fim em seu próprio processo de vir à existência. De modo que aplicar

> meios intrinsecamente maus para alcançar um fim intrinsecamente bom é um simples absurdo e um fracasso. – Jacques Maritain, *Man and The State*.

Um método simples para entender a diferença entre o estado e a sociedade é analisar seus meios e fins.

O fim de um estado é regular a sociedade para manter sua existência e fazer valer seus privilégios. Seu privilégio primordial é o monopólio do exercício da violência sobre as pessoas e propriedades dentro de um território definido. O estado usa a força na forma de lei ou a ameaça da lei para impor suas políticas. Atrás de cada lei está uma arma com a possibilidade de irromper violência se a lei não for obedecida. No entanto, o estado prefere obter a complacência do que ter de punir alguém, porque a punição é um processo desajeitado que pode inspirar resistência. O estado prioriza a aquisição de riqueza porque não produz nada e não tem receita, exceto o que é derivado de outros por meio de ameaças ou violência. Em outras palavras, aqueles que estão no poder usam o monopólio da força como meio de criar e sustentar o privilégio desejado.

A sociedade é a interação voluntária dos indivíduos com as instituições que evoluem das associações. Uma instituição é um costume, padrão de comportamento ou relacionamento dentro da dinâmica de uma sociedade; casamento, igreja ou a família são exemplos. O dinheiro é uma instituição vital tanto para o estado quanto para a sociedade.

O objetivo da sociedade – se é que se pode dizer que uma rede altamente descentralizada tem um propósito consciente – é ser um local no qual os indivíduos possam trocar por benefício mútuo, seja esse benefício definido em termos econômicos, espirituais ou outros. A sociedade é voluntária, com obrigações legais decorrentes apenas de consentimento e contrato. Este é o meio social: a livre associação. O fim ou objetivo da sociedade é expresso por cada membro que age em seu próprio interesse. Como os indivíduos são diversos e imprevisíveis, a forma da sociedade é fluida e imprevisível, exceto por não ser violenta.

“A forma segue a função” significa que a forma básica de qualquer coisa é determinada pelo seu propósito. A forma de uma cadeira é ditada por sua função como estrutura sobre a qual as pessoas se sentam, e é por isso que uma cadeira de sucesso tem uma superfície estável. Para o arquiteto Frank Lloyd Wright, a forma e a função de uma coisa tinham que ser inseparáveis para que sua síntese fosse bem-sucedida. “A forma

segue a função – isso foi mal compreendido”, observa Wright. “Forma e função devem ser uma, unidas em uma união espiritual.” Se os dois estiverem em conflito, então a forma falha ou a função revela-se diferente do que foi declarado. Se manter a paz envolve matar pessoas inocentes, por exemplo, significa que manter a paz não é o fim a ser expresso. Durante a Guerra do Vietnã, um oficial do exército dos EUA justificou o bombardeio de áreas civis na província de Bến Tre, no delta do Mekong, com a declaração: “Tornou-se necessário destruir a cidade para salvá-la”. Essa explicação se transformou no infame ditado: “Tivemos que destruir a vila para salvá-la”. Uma forma e uma função discordantes muitas vezes revelam uma função oculta e verdadeira.

Mahatma Gandhi expressou famosamente a conexão entre forma e função na dinâmica social. “Se cuidarmos dos meios”, escreve ele, “o fim cuidará de si mesmo”. Isso refletia a realidade dos meios serem os fins em andamento. Gandhi não desvaloriza a importância do fim à vista, mas reconhece que cada estágio dos meios deve expressar o fim em uma progressão lógica para que o fim se materialize.

A maioria das pessoas se concentra em objetivos, como prosperidade, e depois descobre como alcançá-los. As estratégias são vistas como pragmáticas e quase intercambiáveis: o que funciona ou oferece um atalho. Mas a crueldade não pode levar a relacionamentos amorosos; só a benevolência pode. O roubo não cria respeito pelos direitos de propriedade; só a honestidade o faz. Se o objetivo das criptomoedas é libertar indivíduos financeiramente, então o meio de alcançá-lo é inseparável desse fim. Os meios são o respeito aos direitos individuais, aos livres mercados, à paz e à sociedade. As estratégias opostas são o coletivismo, os monopólios e a violência, sendo o estado um resultado previsível.

“Deveria haver uma lei” é uma solução instintiva comum para alcançar quase qualquer objetivo social nos dias de hoje; as pessoas clamam por usar a violência institucionalizada do estado, a fim de promulgar leis que punam ou incentivem outros a aceitar um fim desejado que não aceitariam de bom grado. O objetivo pode ser comparativamente modesto, como impor um código de vestimenta pelo qual homens, e não mulheres, ficam de topless. Ou pode ser abrangente como a imposição de uma determinada doutrina religiosa. A reação reflexiva de “deveria haver uma lei” ignora a questão de saber se os meios e os fins estão em conflito. Poucas pessoas perguntam se é mesmo possível que a lei imponha ideias e atitudes, pensamentos e sentimentos; não é. O

máximo que é possível é que a lei intimide as pessoas a expressar externamente pensamentos e sentimentos "corretos", apesar do que pensam e sentem por dentro.

Como tais leis interferem na liberdade de consciência e de expressão de um indivíduo, uma sociedade livre não as impõe; como meio, tais leis contradizem os fins da sociedade. No entanto, por conferirem ao estado imenso poder sobre sua população, tais leis são uma prática padrão para aqueles que estão no poder; como meio, eles atingem os fins desejados. Quanto mais vaga for a declaração de uma meta – "igualdade de renda" ou "justiça social" – mais poder ela confere ao estado, porque a definição é elástica. Com a cripto de livre mercado, o fim está bem definido: uma transferência descentralizada e privada de fundos ou outras informações em uma rede peer-to-peer. Com fiat e o sistema bancário, o fim é subjetivo e aberto à redefinição: estabilidade monetária.

Todo mundo sabe que alguns objetivos exigem meios específicos. Manter-se saudável requer comer bem, praticar exercícios e adotar bons hábitos. Os meios apropriados tornam-se menos óbvios quando o fim é complexo, amorfo ou não expresso com franqueza. De alguma forma, a conexão lógica entre os dois se perde. "Os fins justificam os meios" tornou-se uma desculpa para abandonar as considerações práticas e morais sobre como alcançar objetivos específicos. Uma vez que um fim é estabelecido, um menu de meios é examinado para aqueles que devem atingir o objetivo da forma mais rápida e econômica possível. Questões mais fundamentais sobre a relação entre meios e fins raramente são feitas. A guerra pode realmente trazer a paz? A censura pode criar uma sociedade aberta? A proibição de criptomoedas protege a segurança financeira?

Quando os fins e os meios entram em conflito, o fim torna-se uma impossibilidade prática. Uma pessoa que declara que "os fins justificam os meios" ou está muito equivocada sobre como os objetivos são alcançados, ou tem em mente um objetivo totalmente diferente do que é declarado. A utilização de um meio hostil para a obtenção de um fim introduz um elemento orwelliano. O duplipensar intrínseco no slogan da Primeira Guerra Mundial "Uma guerra para acabar com todas as guerras" é óbvio. Os meios obviamente falharam em atingir o objetivo declarado, porque a eliminação do conflito nunca foi o objetivo real; território, poder e lucro foram o propósito da Primeira Guerra Mundial. O falso objetivo foi aceito, no entanto, e ainda é alardeado, embora não

faça sentido. Ninguém fala de “Uma Verdade para Acabar com Todas as Verdades”, “Um Argumento Lógico para Acabar com Toda a Lógica” ou “Uma Virtude para Acabar com Todas as Virtudes” porque estes são absurdos autocontraditórios. A maneira de acabar com a guerra não é travá-la, mas recusar o engajamento. O meio – travar uma guerra – é diametralmente oposto ao fim declarado – prevenir mais guerra. Quando isso ocorre, é hora de olhar sob a superfície para a intenção real.

Isso revela uma profunda diferença ideológica entre os defensores do estado e os defensores da sociedade ou do livre mercado. Os estatistas são orientados para os fins; defensores da sociedade civil são orientados para os meios. Isso não sugere que a sociedade civil – isto é, os indivíduos dentro dela – não tenha ou estabeleça objetivos específicos. Diz que a sociedade percebe que os meios adequados para atingir qualquer fim devem ser empregados. Em contraste, os estatistas se concentram inteiramente no fim e usam todo e qualquer meio necessário ou conveniente para alcançá-lo.

Os estatistas fornecem um plano detalhado para o que constitui uma sociedade justa, por exemplo. Um fim declarado dessa sociedade pode ser uma igualdade socioeconômica, que exija que o estado monopolize todas as questões monetárias, incluindo o comércio, para garantir a distribuição adequada de riqueza e oportunidades. O fim dita os meios. Isso vale para uma sociedade moral, qualquer que seja a definição de “moralidade” empregada. O fim exige que o estado monitore o comportamento, as palavras e as atitudes expressas por cada indivíduo. Sempre que um fim específico é identificado como um objetivo primordial e independente, então o uso da força torna-se necessário para impô-lo a pessoas que discordam pacificamente, porque alguém sempre o fará.

Em contraste, a abordagem de livre mercado é orientada para os meios. Uma sociedade justa não visa um resultado como um arranjo socioeconômico específico. Quaisquer arranjos que resultem de indivíduos fazendo escolhas livres e pacíficas são considerados justos. O que quer que seja voluntário é justo – ou, pelo menos, tão próximo disso quanto os seres humanos imperfeitos em um mundo imperfeito podem chegar. Por exemplo, uma faculdade particular que discrimine negros e uma que aplique uma política somente para negros existiriam lado a lado no mercado. Desde que ambos sejam financiados por fundos privados e ninguém seja obrigado a participar, ambos os arranjos são justos

e a lei não pode interferir adequadamente. Se as pessoas consideram as políticas escolares imorais, elas são livres para usar uma ampla variedade de meios pacíficos para promover mudanças. Essas estratégias incluem educação, protesto, piquetes, boicote e persuasão moral. O que eles não podem fazer é usar a força para ditar a maneira como as faculdades usam seu próprio dinheiro para estabelecer suas próprias políticas. A liberdade de associação exige o direito de discriminar.

Os estatistas não são igualmente restritos. Sua primeira escolha ao buscar "reformar" uma prática pacífica, mas imoral, é aplicar a força institucional da lei.

O filósofo francês do século XX, Jacques Maritain, considerou o "o dilema dos meios versus os fins" como o problema da filosofia política. A Revolução Francesa forneceu a ele o modelo de como um fim falhou miseravelmente porque os meios usados para alcançá-lo eram "intrinsecamente maus". Em uma revolução estereotipada, os indivíduos se levantam em massa para tomar o poder da elite e dos governantes opressores. As revoluções são chamadas de "populares" porque começam com uma onda de resistência popular contra o status quo. E é verdade; é assim que muitas revoluções começam. E então elas se desenrolam de maneira terrivelmente errada. A França foi de uma monarquia absoluta, que devastou os direitos das pessoas comuns, à "uma pessoa superior chamada estado Nação", que devastou os direitos das pessoas comuns. A prometida "Liberté, Égalité, Fraternité" (Liberdade, Igualdade, Fraternidade) nunca se materializou. Em vez disso, autocratas sanguinários como Robespierre e Saint-Just, juntamente com uma nova classe de burocratas mesquinhos, realizaram prisões e execuções em massa que geralmente visavam pessoas comuns que violavam as leis econômicas – contrabando, por exemplo.

A Revolução Bolchevique é outra lição de moral. O catastrófico número de mortos e fome causados pelo envolvimento da Rússia na Primeira Guerra Mundial, mais do que um compromisso com o marxismo, levou os russos à revolta. As terceiras partes confiáveis chamadas "líderes" levaram a sociedade longe demais, e eles perderam toda a confiança. Seu colapso deixou um vazio de poder. Sob o lema "Paz, Pão e Terra", oficiais revolucionários correram para preencher esse vazio com um regime totalitário e dogmático, em vez do paraíso dos trabalhadores que eles mesmos haviam prometido. É o caminho desgastado das revoluções; conheça o novo chefe, igual ao antigo chefe.

Essas revoluções não atingiram "o objetivo final e a tarefa mais essencial do corpo político ou da sociedade política", explica Maritain. A tarefa era "melhorar as condições da própria vida humana" e "procurar o bem comum da multidão, de tal maneira que cada pessoa concreta, não apenas em uma classe privilegiada [...] pudesse verdadeiramente alcançar essa medida de independência que é própria à vida civilizada". Em termos coloquiais, Maritain está dizendo: "você não pode chegar lá a partir daqui".

Por quê? Porque os líderes revolucionários se tornaram um novo conjunto de terceiras partes confiáveis. Os revolucionários formaram uma nova elite, que adotou a mesma estrutura básica de poder de antes: governo absoluto que governa por meio de reivindicações de legitimidade, intimidação e força bruta. Mudaram-se os rostos, as ideologias e os fins declarados, mas não os meios de poder centralizado que se impunham pela força institucionalizada. Os revolucionários usaram os mesmos meios que seus predecessores, e chegaram aos mesmos resultados: a opressão das pessoas comuns. Somente se mudando os meios – apenas descentralizando o poder de volta para o indivíduo – uma revolução pode evitar se transformar em só mais um estado. Somente quando os líderes revolucionários deixarem de evoluir para uma terceira parte confiável, que um Robespierre, um Lenin, um Pinochet, um Mao ou um Castro deixarão de ser inevitáveis.

A revolução das criptomoedas resolve o Dilema Meios Versus Fins dentro da filosofia política, porque as criptomoedas são o meio e o fim ao mesmo tempo. Gandhi também afirma: "Não há muro de separação entre meios e fins. Meio e fim são termos sinônimos em minha filosofia de vida." Eis a estratégia das criptomoedas: descentralizar as trocas financeiras por meio de uma blockchain, a fim de contornar terceiras partes confiáveis e devolver o controle monetário ao indivíduo. O fim político: descentralizar as trocas financeiras para contornar terceiras partes confiáveis e devolver o controle monetário ao indivíduo. O meio e o fim são um no mesmo. O processo pseudônimo, descentralizado e peer-to-peer é transformador. Quando a flexão do poder individual se torna suficientemente difundida, torna-se uma revolução sem líder – uma revolução independente de confiança – que depende de indivíduos perseguindo seus próprios interesses. Os meios são "qualquer coisa que seja pacífica". O fim é o que resulta dos meios.

O estado Contra a Sociedade

Em sua obra clássica, *The State* (1914), o sociólogo alemão Franz Oppenheimer encabeça uma análise dos dois termos mais importantes na discussão política: "o estado" e "a sociedade". Os termos antitéticos, cada qual expressa um modo de organização humana e cada um reflete a importância da riqueza ou produtividade para a existência humana. A condição natural do homem é a pobreza. Um bebê nasce com nada além de seu próprio desamparo, e morrerá sem a intervenção tenaz de um cuidador. Uma vez que uma pessoa é capaz de usar seu trabalho para transformar recursos ou criá-los, então ela é capaz de cuidar de si mesma através de um esforço contínuo. A produção de riqueza é literalmente o que permite que as pessoas sustentem suas vidas. A habilidade de produzir e controlar a riqueza é uma questão de vida ou morte.

Oppenheimer identifica dois meios antagônicos pelos quais a riqueza é controlada: o estado e a sociedade. Ele define o estado como "a soma de privilégios e posições dominantes que são criadas pelo poder extraeconômico". As palavras "poder extraeconômico" significam força ou ameaça de força. As instituições do estado incluem os militares, a imposição da lei, as legislaturas e as burocracias. Seu denominador comum é a administração e manutenção do poder estatal através do uso da violência institucionalizada. "Eu defino o estado", escreve Rothbard, "como aquela instituição que possui uma ou ambas (quase sempre ambas) das seguintes propriedades: (1) adquire sua renda pela coerção física, conhecida como 'tributação'; e (2) afirma e geralmente obtém o monopólio coagido da prestação de serviços de defesa (polícia e tribunais) sobre uma determinada área territorial. Uma instituição que não possua nenhuma dessas propriedades não é e não pode ser, de acordo com minha definição, um estado".

Oppenheimer define a sociedade como "a totalidade de conceitos de todas as relações e instituições puramente naturais entre homem e homem". As palavras "puramente natural" significam "voluntário", sendo a sociedade a soma total das interações pacíficas dos indivíduos dentro dela. As instituições da sociedade incluem o livre mercado, os locais de adoração, as escolas, as instituições de caridade e as artes. Rothbard descreve a sociedade como um lugar "onde não há possibilidade legal de agressão coercitiva contra a pessoa ou propriedade de um indivíduo". Os anarquistas se opõem ao estado porque ele tem seu próprio ser em tal agressão, a saber, a expropriação da propriedade privada

por meio de impostos, a exclusão coercitiva de outros prestadores de serviços de defesa de seu território e todas as outras depredações e coerções que são construídas sobre esses focos gêmeos de invasões de direitos individuais". O estado é chamado de esfera pública; a sociedade é a esfera privada.

(Nota: O estado e a sociedade são abstrações, e deve-se tomar cuidado para não torná-los em algo excessivamente concreto. A abordagem analítica do liberalismo clássico é o individualismo metodológico, que afirma que apenas os indivíduos existem e agem. Todas as instituições – incluindo as de ambos o estado e a sociedade – podem ser reduzidas às ações dos membros individuais de cada instituição).

A riqueza pode ser controlada pelo estado ou pela sociedade – isto é, pelos membros individuais de ambos – mas só pode ser produzida pela sociedade. O estado emprega o que Oppenheimer chama de "meio político" – isto é, força ou ameaça de força – para adquirir a riqueza que não produz nem adquire por meio de troca voluntária. A riqueza é retirada de pessoas que produzem e trocam, o que Oppenheimer chama de "meio econômico" de adquirir bens.

O estado não costuma tomar a riqueza pela força bruta, no entanto. Em vez disso, o estado usa métodos de roubo mais sutis e menos arriscados. Por exemplo, canaliza a produtividade da sociedade para uma forma de dinheiro que monopoliza ao emiti-lo e impõe leis de curso legal. Então, o monopólio monetário é consolidado regulando as instituições financeiras através das quais o dinheiro é forçado a fluir. Isso permite que o estado realize roubos sutis, como a inflação. A violência direta é o monopólio monetário, que proíbe e pune os concorrentes do livre mercado.

Expresso de outra forma: O fim do estado é manter sua existência e poder. Para cumprir esse objetivo, o estado precisa da riqueza e da cooperação da sociedade, pois não produz riqueza. O estado precisa roubar da sociedade porque sua única fonte de "renda" é o que ele obtém através de meios que incluem impostos, confiscos, multas, taxas, tarifas, inflação e subornos. A força e as ameaças de força são os meios necessários – os meios políticos –: os meios do estado.

Em contraste, a sociedade não tem fins. Embora seja um motor de criação e troca, a sociedade não tem consenso sobre quais devem ser os resultados dessa produtividade. Cada membro individual age para perseguir seu interesse próprio, com cada pessoa tendo uma definição única do que compreende esse objetivo. O objetivo de uma pessoa pode

ser ganhar um milhão de dólares, enquanto o de outra pode ser adquirir educação. O meio pelo qual cada indivíduo atinge seu objetivo é através da criação e do comércio – os meios econômicos – que produzem sua própria versão de riqueza. Novamente, o que constitui riqueza difere de pessoa para pessoa, e inclui dinheiro, cultura, conhecimento, família, espiritualidade e todos os outros valores humanos possíveis. Os meios da sociedade são o oposto da coerção, porque uma troca ocorre apenas quando todas as partes de uma transação concordam com seus termos e todas as partes se beneficiam.

Rothbard destaca a principal diferença entre interagir com a sociedade e com o estado.

> Se eu deixar ou me abster de comprar cereais no mercado, os produtores de cereais não virão atrás de mim com uma arma ou ameaça de prisão para me obrigar a comprar; se eu não conseguir entrar na American Philosophical Association, a associação não pode me forçar a entrar ou me impedir de desistir de minha filiação. Somente o estado pode fazê-lo; só o estado pode confiscar minha propriedade ou me colocar na cadeia se eu não pagar seus impostos.

A principal diferença é o consentimento.

O individualista americano Albert Jay Nock foi o principal condutor do pensamento de Oppenheimer para os Estados Unidos. Ele capturou o sentimento central de seu mentor no livro *Our Enemy, The State*, no qual Nock observa: "Tomando o estado, onde quer que seja encontrado, adentrando em sua história a qualquer momento, não se vê como diferenciar as atividades de seus fundadores, administradores e beneficiários daqueles de uma classe criminosa profissional".

A perspectiva de "adentrar a história do estado" atraiu muitos teóricos políticos, porque se relaciona diretamente com a natureza do estado e se ele é legítimo. Por sua vez, isso aborda a questão de porque as pessoas obedecem ao estado. Muitas pessoas parecem consentir com a presença do estado, enquanto reclamam sobre quão corrupto é o sistema e os padrões duplos na lei. Mesmo aqueles que consideram a maioria das leis injustas parecem acatá-las, mesmo não sendo explicitamente forçados a fazê-lo. Mas por quê?

Examinar as raízes do estado é o ponto de partida de uma resposta. Em geral, existem quatro teorias básicas e às vezes sobrepostas

de como um estado se origina. Cada teoria traz implicações diferentes para a relação do estado com a sociedade e a legitimidade que reivindica.

A primeira teoria é sobrenatural. Sustenta que o estado existe pela vontade de Deus ou algo equivalente. Este é o direito divino de reis ou governantes, e a teoria muitas vezes resulta em uma teocracia. Membros menores da sociedade – que presumivelmente também são colocados em suas posições por Deus – devem lealdade aos líderes ungidos, como parte de seu dever para com Deus. Uma igreja estabelecida às vezes atua como um braço do estado, com líderes religiosos reforçando a legitimidade divina do governante.

A segunda teoria de como um estado se origina baseia-se em uma explicação mais naturalista. O estado é uma instituição espontânea que surge do ato da comunidade, argumenta-se. A pessoa e a propriedade dos indivíduos exigem proteção, e seus contratos exigem um mecanismo de execução. Isso faz com que uma autoridade superior evolua para prestar os serviços necessários, atuando como policial e árbitro de disputas. A sociedade paga ao estado da mesma maneira que paga a um empreiteiro pela prestação de um serviço valioso. De acordo com a teoria do consentimento, nenhuma linha rígida distingue o estado da sociedade, porque ambos estão engajados em um empreendimento cooperativo.

A terceira e quarta teorias envolvem conflito. A terceira teoria afirma que o estado surge devido à guerra interna dentro de uma sociedade. Karl Marx popularizou essa visão, analisando o estado como parte da luta de classes, através da qual os capitalistas controlam e exploram os trabalhadores; isto é, os capitalistas usam o estado – ou se unem ao estado – para oprimir os trabalhadores. Para Marx, o estado expressa e protege uma classe da sociedade às custas de outra, e esta não deve qualquer lealdade a seus opressores. De fato, o dever dos trabalhadores é resistir e se rebelar.

A quarta teoria das origens do estado aponta para conflitos externos em que uma tribo conquista outra. A tribo vitoriosa forma a classe alta dentro da sociedade resultante, e a tribo conquistada paga tributo por meio de obediência e riqueza.

Dentro do liberalismo clássico, as duas teorias que lutaram pelo domínio são a teoria do consentimento, pela qual o estado evolui naturalmente a partir das necessidades da sociedade, e a teoria da conquista, pela qual o estado está em constante guerra contra a(s) classe(s) não

privilegiada(s) da sociedade. Estas não são apenas suposições históricas. São também abordagens analíticas para se o estado pode ou não reivindicar legitimidade.

As teorias do consentimento e da conquista do estado

Se o estado governa com o consentimento da sociedade e fornece um serviço necessário, então o argumento contra a revolução – na forma das criptomoedas ou em nome de qualquer outra coisa – é consideravelmente enfraquecido. É provável que o sistema monetário seja visto como necessitando de uma reforma considerável, em vez de ser eliminado.

Na teoria do consentimento do estado, o filósofo inglês do século XVII John Locke se destaca por meio de seus *Dois Tratados sobre o Governo*. A filósofa americana contemporânea Karen Vaughn observa a partir de seu *Segundo Tratado*: "Locke argumenta o caso dos direitos naturais individuais, o governo limitado dependendo do consentimento dos governados, separação de poderes dentro do governo e, mais radicalmente, o direito das pessoas dentro da sociedade de depor governantes que não cumprem sua parte no contrato social". O trabalho de Locke, sobre o qual as revoluções francesa e americana se basearam, continua sendo uma pedra de toque da teoria do consentimento para o governo limitado dentro do liberalismo clássico.

Locke acredita que Deus deu o mundo a todos os homens em comum e justifica a propriedade privada – a apropriação de um bem comum para uso pessoal – argumentando que cada homem tem um direito de propriedade sobre sua própria pessoa. Com base na autopropriedade, Locke argumenta: "O trabalho de seu corpo e o trabalho de suas mãos, podemos dizer, são propriamente dele. O que quer que ele remova do estado que a natureza forneceu e o deixou, ele misturou seu trabalho e juntou a ele algo que é seu, e assim o torna sua propriedade". Até agora, isso não parece sugerir que o estado, ao contrário dos indivíduos, produza riqueza ou valor.

Locke então postula que a necessidade de proteger "vida, liberdade e propriedade" leva os homens a formar um governo. Uma das principais razões pelas quais o estado surge é como um escudo contra a confusão quanto aos títulos de propriedade e outros conflitos, que ocorrem quando os indivíduos acumulam e competem por riqueza em um

mundo de escassez. Por meio de um contrato social explícito, os homens dão ao estado o direito de julgar as disputas. De sua parte, o estado se compromete a garantir a reivindicação de propriedade dos homens – por meio de leis de herança, por exemplo. Locke rejeita a afirmação de que o consentimento prestado ao estado pelos membros iniciais da sociedade pode vincular as gerações futuras, no entanto. Em vez disso, ele desenvolve uma doutrina de consentimento tácito pela qual as pessoas que não consentiram explicitamente ainda são obrigadas a aceitar a autoridade do estado. Diz-se que cada pessoa que vive em sociedade e desfruta de seus benefícios concorda com as regras pelas quais um estado limitado governa.

A retirada do consentimento tácito é possível. Um homem pode renunciar a sua propriedade e deixar a comunidade. Enquanto ele permanecer, no entanto, ele aceita implicitamente a autoridade do estado. Afinal, como argumenta Locke, o "bom título" de sua propriedade veio do estado, que facilitou sua justa transferência. Um argumento semelhante pode ser feito sobre a riqueza acumulada em virtude de um contrato: o contrato tem validade devido ao contexto legal fornecido pelo estado. Somente quando o estado deixa de cumprir sua parte no contrato social é que se justifica a rebelião contra sua autoridade. Caso contrário, o estado e a sociedade são parceiros.

A teoria da conquista do estado contrasta fortemente com o modelo lockeano e é a teoria preferida pelos anarquistas individualistas. Ele tenta fundamentar o estado primitivo em fatos históricos, em vez de conjecturas políticas. Uma expressão comum da teoria da conquista é a seguinte: tribos agrícolas se estabelecem e se tornam dependentes de áreas específicas de terra. Nômades itinerantes fazem guerra às tribos mais sedentárias pelos benefícios econômicos que vêm da pilhagem e do saque. Os nômades começam matando e arrasando, mas descobrem que é do seu interesse econômico de longo prazo escravizar e exigir tributos. Por que roubar por uma única estação quando é possível roubar para sempre? Este é o modelo de conquista simplista para explicar como surgiu o estado e sua relação com a sociedade.

Em *Our Enemy, The State*, Nock defende a teoria da conquista do estado em bases históricas. Em *For A New Liberty*, Rothbard apresenta uma versão modificada da teoria. Ele afirma que a conquista foi a gênese típica do estado, mas admite que alguns estados podem ter evoluído de maneira diferente. Mas mesmo um estado que emergiu de um

contrato social explícito, argumenta ele, não poderia vincular novas gerações por meio de consentimento tácito, porque uma atribuição de direitos naturais requer um contrato explícito. Como não existe renovação geracional do contrato, qualquer estado atual não tem legitimidade.

Ao defender a teoria da conquista, tanto Nock quanto Rothbard se apoiam fortemente em Oppenheimer, que sustenta que o estado consiste em pessoas que desejam satisfazer seu “impulso econômico” através dos meios políticos – através do uso da força. Oppenheimer postula seis estágios pelos quais um grupo conquistador normalmente passa para se tornar um estado:

- Primeiro, um grupo guerreiro ataca e saqueia uma comunidade vulnerável para roubar riqueza em vez de produzi-la por conta própria. Os ataques vikings na costa britânica são um exemplo.
- Em segundo lugar, a comunidade vitimizada deixa de resistir ativamente; às vezes é feito um acordo explícito entre os agressores e as vítimas. Os saqueadores passam a saquear apenas o excedente, deixando suas vítimas vivas e com comida suficiente para garantir a produção de riqueza futura a ser saqueada repetidamente. Eventualmente, os dois grupos reconhecem interesses mútuos, como proteger as plantações de terceiras partes externas.
- Terceiro, as vítimas prestam homenagem aos invasores, eliminando a necessidade de qualquer violência.
- Quarto, os dois grupos se fundem territorialmente e vivem juntos na mesma área.
- Quinto, o grupo belicoso assume a autoridade para arbitrar disputas, o que envolve o monopólio do uso da força.

Oppenheimer descreve o último estágio em que ambos os grupos desenvolvem o “hábito de governar”. Em seu capítulo “A Gênese do Estado”, ele explica: “Os dois grupos, separados, para começar, e depois unidos em um território, são inicialmente apenas colocados um ao lado do outro, depois são desmembrados um pelo outro. Misturam-se, unem-se, amalgamam-se à unidade, nos costumes e hábitos, na fala e no culto. Logo os laços de relacionamento unem os estratos superiores e inferiores.” Os estratos superiores eram chamados de “classe de mestres.”

O estado, que se originou da conquista externa, evolui para uma agência de conquista interna pela qual as camadas superiores do estado

utilizam os meios políticos para se beneficiar economicamente às custas das camadas inferiores de produtores. Nessa visão, o estado surge e se mantém como parasita e inimigo da sociedade. Ainda assim, em qualquer que seja o caminho que leve ao surgimento de um estado uma questão permanece: por que as pessoas aceitam a autoridade do estado sobre suas vidas, suas propriedades e o futuro de suas famílias?

Servidão Voluntária

A força é geralmente o último recurso que o estado introduz quando outros métodos de persuasão, como o apelo ao patriotismo, não funcionam. Afinal, a presença da força aberta poderia colocar em questão a legitimidade do estado. Para evitar a desobediência ou a rebelião, o estado tenta justificar-se aos olhos da sociedade para que possa garantir as vantagens da violência sem incorrer em seus perigos. Nenhuma análise da relação entre estado e sociedade está completa sem examinar a questão da legitimidade.

Um ensaio do século XVI intitulado “Discurso da Servidão Voluntária” do jurista francês Étienne de La Boétie é uma discussão inicial de uma questão inquietante. Por que as pessoas obedecem a leis injustas? La Boétie pergunta: “Se um tirano é um homem e seus súditos são muitos, por que eles consentem em sua própria escravização?” Corretamente ou não, La Boétie não acredita que o estado governe principalmente pela força. Afinal, há muito mais pessoas na sociedade do que agentes do estado. Se mesmo uma pequena porcentagem da população se recusa a obedecer a uma lei, então a lei se torna inaplicável; a tirania é automaticamente derrotada se as pessoas retirarem seu consentimento. No entanto, a maioria das pessoas obedece sem ser forçada a fazê-lo. La Boétie desenvolve uma explicação; ele chama isso de “servidão voluntária”.

O Discurso circulou pela primeira vez privadamente na França (por volta de 1553) em um cenário de guerra estrangeira e conflito interno. Os estados-nação europeus estavam em ascensão, e os monarcas entraram em conflito não apenas entre si, mas também com seus próprios cidadãos, de quem exigiam muito dinheiro e obediência. O século XVI deu origem à tirania que levou à Revolução Francesa séculos depois.

Nascido em uma família abastada e politicamente conectada, La Boétie escapou do analfabetismo, miséria e doenças que se abateram

sobre a maioria de seus compatriotas. A fome era tão comum na França que os homens esculpiam cruzes no pão recém-assado para simbolizar a sacralidade da comida. Pragas irromperam repetidamente. Enquanto o camponês lutava para sobreviver, os impostos estaduais consumiam um terço ou mais de sua renda, com os dízimos da igreja absorvendo outro décimo. Grupos itinerantes de soldados roubavam à vontade e sequestravam filhos jovens para preencher suas fileiras. A França era uma monarquia absoluta, o que significava que o poder nacional não era distribuído, mas ficava com o rei e era administrado por meio de nomeações. Para arrecadar dinheiro para a guerra e o luxo, o rei vendia títulos aos "nouveau riche", que formavam uma nova aristocracia com notório desprezo pelas classes mais baixas. Enquanto isso, as fileiras de advogados aumentavam enquanto administravam burocracias para alimentar o apetite de um estado em crescimento.

Por que o homem comum obedeceu a um sistema que o tratou tão miseravelmente e foi claramente manipulado contra ele? Para garantir isso, o monarca foi ungido por Deus e abençoado pela Igreja Católica dominante, mas a ascensão do protestantismo na França – os huguenotes – fez com que um segmento crescente da sociedade não reconhecesse a divindade do rei. Havia também lealdades provinciais que competiam com as nacionais. A maioria dos franceses dava fidelidade primária à província de seu nascimento e não à nação ou ao rei, e as províncias variavam amplamente em costumes, práticas religiosas e linguagem. Essas diferenças dividiram a nação. Também e com razão, o rei temia que potências estrangeiras se alinhassem contra ele com províncias rebeldes. Uma tempestade perfeita entre o estado e a sociedade parecia estar se formando.

O Discurso provavelmente foi escrito enquanto La Boétie era estudante de direito na Universidade de Orléans, famosa pela atividade huguenote. De fato, um de seus professores seria mais tarde queimado na fogueira por heresia. O ensaio em si era uma resposta a um evento específico – a Revolta de Gabelle em Bordeaux. O Gabelle era um imposto muito odiado sobre o sal, que não era apenas uma necessidade humana, mas também um monopólio estatal. Os manifestantes mataram o diretor geral do Gabelle junto com dois de seus oficiais. Em retaliação, 140 plebeus foram mortos, muitos outros foram chicoteados e multas exorbitantes foram impostas.

La Boétie era um observador perspicaz da sociedade. Quando o povo finalmente se rebelou, ele observou e se perguntou por que o estado foi capaz de fazer quase tudo o que queria por tanto tempo, não importa o quão tirânico. Ele assistiu de perto também depois que a Revolta de Gabelle foi anulada. Por que as pessoas não se levantaram novamente, ele se perguntou, desta vez en masse? Por que a sociedade tolerava o estado? *O Discurso* foi a resposta de La Boétie.

Nele, o autor conclui que a obediência coletiva da sociedade vem de “um vício para o qual nenhum termo pode ser encontrado suficientemente vil, que a própria natureza repudia e nossas línguas se recusam a nomear”. Ele chama isso de “servidão voluntária”. É um vício porque contradiz a natureza humana; na verdade, até os animais brutos lutam para se libertar quando apanhados em uma armadilha. Cada homem recebe sua própria capacidade de raciocinar, argumenta La Boétie, e a virtude reside no cultivo de cada pessoa de sua própria independência inata. Mas a habilidade do homem de fazê-lo exigiu a morte da tirania, que é a antítese da independência individual. A defesa do tiranicídio não era novidade para a teoria europeia, mas La Boétie adota um viés diferente. A maneira de “matar” um tirano é destruir seu poder através da resistência não-violenta. Dessa maneira, o povo não mata um homem, mas a própria tirania. A liberdade exige apenas que um número suficiente de pessoas retire seu consentimento e cooperação.

> Aquele que assim domina você tem apenas dois olhos, apenas duas mãos, apenas um corpo […]; ele realmente não tem nada mais do que o poder que você confere a ele para destruí-lo. Onde ele conseguiu olhos suficientes para espioná-lo, se você mesmo não os forneceu? Como ele pode ter tantos braços para bater em você, se ele não os empresta contigo? Os pés que pisoteiam suas cidades, de onde ele os tira senão dos teus?

La Boétie dirige-se diretamente ao camponês francês. “Vocês entregam seus corpos ao trabalho duro para que ele [o tirano ou o estado] possa se entregar a seus deleites e chafurdar em seus prazeres imundos; vocês se enfraquecem para torná-lo mais forte e mais poderoso para mantê-los sob controle”. Por que obedecer?

La Boétie explora as principais formas pelas quais os engenheiros estatais consentem com a sociedade.

As gerações que nasceram “sob o jugo e depois foram nutridas e criadas na escravidão” aceitam sua condição como natural. É o caminho do mundo. Assim, La Boétie considera o costume como a primeira explicação da servidão voluntária. As pessoas acreditam que a vida sempre foi assim; a vida sempre será assim; e é preciso um grande esforço para introduzir uma nova visão a eles.

O autor e teórico francês Michel de Montaigne, que era o melhor amigo de La Boétie, dramatizou o incrível poder da tradição em seu ensaio “Do Costume”. Abre com as palavras:

> Parece ter tido uma apreensão correta e verdadeira do poder do costume, quem primeiro inventou a história de uma camponesa que, acostumada a brincar e carregar um bezerro nos braços, e continuando diariamente a fazê-lo como cresceu, obteve isso por costume, que, quando crescido para ser um grande boi, ela ainda era capaz de suportar.

Mas, argumenta La Boétie, algumas pessoas sempre tentarão se livrar “do jugo”, talvez porque “se lembrem de seus ancestrais e de seus antigos costumes”. Conscientes da história, comparam o passado com o presente e ousam ansiar por um futuro melhor. “Estes são os que, tendo suas próprias mentes boas, os treinaram ainda mais pelo estudo e aprendizado. Mesmo que a liberdade tivesse desaparecido inteiramente da terra, tais homens a inventariam”.

Depois que a maioria se acostuma à obediência automática, o principal desafio do tirano é reduzir a dissidência silenciando os poucos que tentam livrar-se do jugo. Dois meios básicos de fazer isso são controlar a imprensa e monopolizar a educação para que as pessoas não comparem o passado com o presente e percebam o quanto mais é possível no futuro. Com um forte controle da informação, o estado pode inculcar a crença de que age em prol do bem-estar público para manter a paz, o patriotismo e a tradição. Pode convencer as pessoas de que incorpora o bem público. A *lavagem cerebral* é outra razão pela qual as pessoas obedecem.

O estado, então, reforça sua imagem maior que a vida por meio de um processo de *mistificação*: isto é, tenta parecer maior do que a mera reunião de seres humanos em suas fileiras. Os governantes se alinham com a religião, são coroados por oficiais da Igreja, realizam cerimônias pomposas, juram proteger a nação, apelam à autoridade de um

documento fundador e assim por diante. Os agentes do estado estão vestidos com uniformes; são construídos monumentos ao poder estatal e aos líderes do passado; os rituais do ofício são ostensivamente exibidos; e manifestações da autoridade do estado, como tribunais, estão alojadas em edifícios imponentes.

Esta é mais uma razão pela qual as pessoas prestam obediência automática: mistificação. Depois que uma imprensa regulamentada e um sistema escolar os convenceu de que a autoridade do governante é legítima, a mistificação do poder do estado os leva um passo adiante.

Eles ficam amedrontados, intimidados e até temerosos.
Algumas pessoas ainda serão difíceis de convencer, no entanto. Aqueles que não obedecerem por costume, lavagem cerebral ou admiração podem muito bem ser comprados. E, assim, o governante também se engaja na generosidade. La Boétie aponta para as distrações patrocinadas pelo estado que servem como "ópios". Fascinado pelo prazer, o povo não percebe sua própria escravização. Outras vezes, os governantes literalmente alimentam o povo distribuindo estoques de alimentos. "E então todos gritam descaradamente: 'Longa vida ao rei!'", comenta La Boétie com desdém. "Os tolos não perceberam que estavam apenas recuperando uma parte de sua própria propriedade, e que seu governante não poderia ter dado a eles o que estavam recebendo sem primeiro tê-lo tirado deles." Ao fornecer pão e circo – bem-estar do estado e distrações populares – as pessoas são *subornadas* para que abdiquem de sua liberdade.

O suborno direto perde importância, no entanto, ao lado de uma forma indireta que La Boétie chama de "a mola mestra e o segredo da dominação, o suporte e a base da tirania". Isso é suborno institucionalizado pelo qual milhões de pessoas são empregadas em empregos estatais e recebem fundos de impostos com os quais pagam suas contas. Esses funcionários do estado "se agarram ao tirano" e oferecem sua lealdade. Alguns funcionários do estado, como policiais, tornam-se as mãos do estado, alcançando toda a sociedade para implementar leis e políticas. Intelectuais apoiados por impostos, como professores universitários, tornam-se as vozes do estado, defendendo suas políticas. Outros ainda, trabalhando como escriturários ou burocratas menores, fazem a máquina diária do estado funcionar.

Ao longo de gerações, uma vasta nova classe de pessoas emerge dos funcionários do estado: pessoas que servem aos governantes em troca de um salário financiado por impostos e outros benefícios. Esses

funcionários públicos destroem voluntariamente sua própria liberdade e a de seus vizinhos. E o fazem sem reflexão porque a força do costume os leva a acreditar que as coisas sempre foram e sempre serão assim.

A solução de La Boétie para a servidão voluntária é que as pessoas retirem seu consentimento e cooperação do estado. La Boétie aconselha o homem comum: "Eu não peço que você coloque as mãos sobre o tirano para derrubá-lo, mas simplesmente que você não o apoie mais; então você o verá, como um grande colosso cujo pedestal foi arrancado, cair de seu próprio peso e quebrar em pedaços." La Boétie é amplamente reconhecido como uma das primeiras vozes de desobediência civil e resistência não-violenta contra a autoridade.

Se ele estiver correto, se a liberdade é um desejo humano natural, então a própria natureza argumenta a lógica de não cooperar com a tirania. Algo dentro dos seres humanos e até dos animais resiste à tensão de uma coleira. Em vez de quebrar a tensão atacando aqueles que detêm os reinados, La Boétie disse às pessoas que deixassem a tensão afrouxar; deixe a ponta da coleira cair. As pessoas devem se recusar a se defender violentamente ou a se submeter.

Eles devem simplesmente dizer "não".

Estado, Sociedade, Obediência e Cripto

Para repetir: os conceitos e realidades de estado, sociedade e obediência são o contexto em que o Bitcoin nasceu e no qual as criptomoedas agora operam. Eles também definirão seu futuro.

O estado deve tirar a riqueza da sociedade para existir. As criptomoedas não são apenas uma nova e rica fonte de riqueza para saquear, mas também uma forte concorrente da fonte atual mais lucrativa do estado: o monopólio monetário. O objetivo do estado é acessar a bonança das criptomoedas *e* preservar o monopólio monetário. Sendo inteiramente orientado para fins, o estado usará todos e quaisquer meios à sua disposição para atingir esse objetivo. As estratégias já em exibição incluem:

Propaganda: as criptomoedas estão ligadas a crimes como terrorismo, resgates e tráfico de seres humanos de uma maneira que faz com que esses crimes pareçam ser os usos predominantes. A ligação serve a pelo menos dois propósitos. Isso cria uma justificativa para o estado agir contra a criptomoedas e reduz qualquer reação indesejada por parte

do público geral. Em vez disso, o público gritará: “Deverá haver uma lei”.

O Uso da Força: Como o próprio estado é uma força institucionalizada, esta é sua estratégia final em situações em que a obediência não pode ser obtida de outras maneiras. E as criptomoedas são irremediavelmente desobedientes. A estratégia de violência ou conquista empregada pelo estado geralmente se acelera por etapas:

- O estado saqueia. A privacidade das transferências de blockchain e o viés antiestatista da comunidade cripto tornam essa opção problemática. Indivíduos e corretoras vulneráveis são atacados e seus fundos são confiscados, mas grande parte das criptomoedas permanece fora de alcance.
- O estado chega a um acordo com usuários de cripto compatíveis. As corretoras centralizadas que concordam em cumprir os regulamentos bancários e os requisitos de relatórios são licenciadas e se tornam corretoras comparsas.
- O estado protege as corretoras de compadres dos concorrentes. Indivíduos que funcionam fora das zonas cripto regulamentadas – e especialmente corretoras descentralizadas – tornam-se alvos. Atacar esses “inimigos externos” beneficia tanto o estado quanto as corretoras obedientes.
- O estado tenta transformar as criptomoedas em um novo tipo de dinheiro fiduciário. Por meio de instituições financeiras, o estado pode imitar a dinâmica das criptomoedas de forma a reproduzir o monopólio monetário de que goza com a moeda fiduciária. Moeda digital que não usa blockchain pode ser oferecida, por exemplo; isso permitirá uma inflação lucrativa e que o estado rastreie todas as transações de volta para um usuário.

Enquanto passa pelos estágios do uso da força, o estado se envolverá em um duplo pensamento ativo, semelhante ao slogan “Uma guerra para acabar com todas as guerras”. As corretoras centralizadas serão apresentadas como forma de garantir a segurança do patrimônio dos usuários, por exemplo, ainda que o maior perigo para a sua riqueza seja o sistema de banco central que as corretoras espelham.

A propaganda contra as criptomoedas não regulamentadas continuará, pois, na presença de alternativas, o estado precisa que o público continue aceitando o monopólio monetário. Muitas pessoas vão fazê-lo

através do costume. Alguns farão isso por causa de lavagem cerebral pela mídia cúmplice que se concentra em qualquer irregularidade dos usuários de criptomoedas. Enquanto isso, o estado mistificará suas próprias atividades, auxiliado pelo fato de que poucas pessoas entendem a tecnologia das criptomoedas ou da moeda digital. O primeiro – se não regulamentado – será diminuído como inseguro, criminoso e falso. O último – sob controle do estado – será considerado seguro, legítimo e forte.

As criptomoedas que se recusarem a serem regulamentadas continuarão sendo o dinheiro da sociedade – ou seja, o dinheiro de indivíduos que interagem livremente e em seu próprio interesse para benefício mútuo. Continuarão a produzir riqueza. Em virtude da cripto ser orientada para os meios, como a sociedade, ela evoluirá para diversos fins com apenas os meios sendo previsíveis: não-violência e consentimento. O conflito entre dinheiro privado e dinheiro fiduciário persistirá porque os dois têm dinâmicas fundamentalmente antagônicas que se ameaçam. Um dos principais campos de batalha será a opinião pública.

Nesse campo de batalha, o maior desafio que o mundo cripto enfrenta é convencer um número suficiente de pessoas a simplesmente dizer “não”.

Teoria Cripto de Classe e Lei de Livre Mercado

A teoria de classe fundamenta o livre mercado e as criptomoedas: o estado versus a sociedade. O Bitcoin foi projetado para contornar um sistema bancário central que serve à classe política em detrimento da econômica. Como inimiga do estado, a criptomoeda é uma aliada da sociedade.

Guerra de Classes e Cripto

Muitas pessoas assumem que qualquer coisa relacionada a bancos e finanças expressa os interesses de classe dos capitalistas versus o homem comum. O oposto é verdadeiro, mas a confusão é compreensível. A palavra "capitalismo" é comumente aplicada ao capitalismo de compadrio nos dias de hoje – isto é, um arranjo econômico pelo qual algumas empresas desfrutam de um relacionamento próximo e mutuamente benéfico com funcionários do estado e recebem tratamento privilegiado. Um "capitalista" tradicional é aquele que possui e usa bens de capital, permanecendo na sociedade sem vínculo com o estado; esse arranjo econômico às vezes é chamado de "capitalismo laissez-faire". É uma expressão do livre mercado e é um benefício para o homem comum, porque o capitalismo laissez-faire atua como um motor de prosperidade.

Os bancos centrais e a maioria das instituições financeiras expressam o capitalismo de compadrio. O capitalismo laissez-faire expressa o livre mercado. Assim, uma afirmação mais específica do conflito de classes é o capitalismo de estado e compadrio versus sociedade e capitalismo laissez-faire. Nesse conflito, a criptomoeda cai claramente do lado da sociedade. A lealdade de classe da criptomoeda é evidente pelos notáveis paralelos entre sua forma e função e os da sociedade. Os paralelos incluem:

- O indivíduo é o locus do poder.
- Ambos são descentralizados até o nível do indivíduo.
- Voluntarismo é o modo de operação.
- Sua finalidade é facilitar as trocas, principalmente econômicas.
- As trocas ocorrem somente com o consentimento de todos os envolvidos.

- Terceiras partes confiáveis são desnecessárias.
- A privacidade é preservada, caso os participantes assim o desejem.
- Não há barreira artificial à entrada.
- Nenhum deles é detentor de um ponto fraco em que todo o sistema esteja vulnerável.
- A riqueza está sendo constantemente criada.
- Riqueza e status são baseados em labuta.
- As trocas não são baseadas em ideologia ou política.
- Reputações são importantes.
- O estado é o inimigo da classe.

Por outro lado, a forma e a função do estado são antitéticas à criptomoeda e ao livre mercado.

- O estado é o locus do poder.
- Todo o poder é centralizado em burocracias.
- A coerção é seu modo de operação.
- O objetivo do estado é manter sua própria existência.
- Transferências forçadas de riqueza e poder são feitas em benefício do estado.
- É a terceira parte última.
- A privacidade é desaprovada e prejudicada a cada passo.
- Barreiras à entrada são erguidas, às vezes chegando a proibições.
- Quem está no poder é o ponto fraco do sistema.
- Nenhuma riqueza é criada.
- Riqueza e poder são baseados na política.
- A riqueza é acumulada por meio de roubo e privilégio.
- A reputação não é necessária e menos importante que o status.
- A sociedade é a inimiga da classe.

Outro teste decisivo para saber se a criptomoeda serve ao estado ou à sociedade está enraizado nas respostas a duas perguntas sobre dinheiro. #1. Quem o emite? O dinheiro fiduciário é emitido pelo estado ou por uma autoridade controlada pelo estado, sendo a concorrência proibida por lei. As criptomoedas são emitidas por empreendedores que

competem vigorosamente entre si pela aceitação popular. #2. As pessoas podem optar por usar a moeda ou não? O estado exige que as pessoas aceitem seu fiat como moeda legal. A cripto deixa a decisão para o indivíduo.

Talvez a maior ameaça à criptomoeda não regulamentada seja o esforço do estado para mudar a forma e a função da criptomoeda para que ela não mais expresse e enriqueça a sociedade, mas expresse e enriqueça o estado. O estado queria esculpir a criptomoeda em sua própria imagem por meio de emissão estatal, regulamentação e outras medidas para que se tornasse um tipo de criptomoeda fiduciária. Isso não pode ser feito; a blockchain não pode ser centralizada sob uma única autoridade. Nenhuma mistura de forças inerentemente antagônicas é possível. Não é sequer claro que criptos estatais e de livre mercado possam coexistir.

O estado continuará tentando forjar uma criptografia bastarda, no entanto, até que esteja convencido de que os esforços são inúteis. Neste ponto, a criptomoeda deixará de ser vista como uma oportunidade e será vista como um perigo. A própria existência de criptomoedas de livre mercado invade uma fonte insubstituível de poder estatal – a emissão de dinheiro. A criptomoeda tem a capacidade de enfraquecer essa fonte de poder e, talvez, destruí-la.

Os recursos de criptografia que enfraquecem o estado incluem:

- As transferências peer-to-peer negam riqueza evitando os bancos centrais através dos quais o fluxo financeiro é controlado.
- A privacidade cripto atrapalha a campanha de controle social do estado. Os dados das instituições financeiras que informam sobre seus clientes são vitais para a capacidade do Estado de impor controle social e econômico.
- A privacidade também evita a centralização do estado. O estado quase pode ser definido como a centralização do poder para beneficiar a elite.
- A existência da cripto levanta a questão de saber se o estado é necessário. Se o livre mercado pode assumir tão facilmente uma função essencial do estado – a emissão e circulação de moeda – então por que não pode assumir outras, ou todas?

A cripto é o dinheiro da sociedade; não pode e não serve ao estado.

A aplicação da lei como ferramenta da guerra de classes

> O poder tributário coercitivo do governo cria necessariamente duas classes: os que criam e os que consomem a riqueza expropriada e transferida por esse poder. Aqueles que criam a riqueza naturalmente querem mantê-la e dedicá-la aos seus próprios propósitos. Aqueles que desejam expropriar procuram formas cada vez mais inteligentes de adquiri-lo sem incitar resistências. Uma dessas formas é a divulgação de uma elaborada ideologia de estatismo, que ensina que as pessoas são o estado e que, portanto, eles só estão pagando a si mesmos quando pagam impostos. Os oficiais do estado e os intelectuais do tribunal nas universidades e os meios de comunicação fazem de tudo para que as pessoas acreditem nessa história fantástica, incluindo a criação de escolas. Infelizmente, a maioria das pessoas passa a acreditar.
> – Sheldon Richman

Uma das armas mais poderosas que o estado possui na luta de classes que trava contra a sociedade é a imposição da lei, incluindo a legislação e o sistema judicial através do qual o estado afirma seus privilégios de classe. A lei é parte integrante do monopólio do estado sobre a força e sua capacidade de coagir a transferência de riqueza da sociedade para suas próprias mãos. Sem o monopólio da imposição da lei, é difícil imaginar como o estado poderia vencer o conflito de classes, porque a sociedade desfruta das enormes vantagens de ser produtiva, inovadora e enérgica.

O estado investe imenso tempo e imensas quantias de dinheiro para convencer a sociedade de que a imposição da lei é uma proteção, não uma ameaça. À medida que um estado se aproxima do totalitarismo, porém, torna-se mais difícil manter esse engano porque suas armas – isto é, as indústrias de imposição da lei – tornam-se mais visíveis.

Uma das últimas ferramentas que o Estado usa para manter a legitimidade antes de começar a usar armas é o argumento N.H.A: não há alternativa. O estado incita o medo de um terrível inimigo – terroristas,

talvez – e então assegura à sociedade que são necessários guardas armados nos aeroportos, câmeras de vigilância e uma força policial militarizada. Além disso, não há alternativa. Ou melhor, a única alternativa é o terrorismo. Muitos acreditarão nessa falsa escolha e aceitarão o menor de dois males.

Felizmente, existe uma alternativa: a lei do livre mercado.

Lei de livre mercado

> Há uma distinção importante entre legislação e lei. Legislação é a lei que vem da ação política. [...] A lei é mais geral no sentido de que a legislação é uma forma de lei, mas a lei também pode ser o tipo de lei que evolui através da interação humana. Na Inglaterra e nos Estados Unidos, muitas vezes somos chamados de países de 'common law' e isso porque uma boa parte e, de fato, a maior parte de nossa lei surgiu por meio de um processo evolutivo que não envolveu a ação de representantes políticos.
> – John Hasnas

Deveria haver uma lei. O significado desta afirmação depende da definição de "lei". O estado trata a palavra como sinônimo de legislação ou lei estatutária, que é a lei que resulta de um processo político. Qualquer pessoa ou grupo que detenha poder suficiente pode aprovar legislação e usar a aplicação da lei para impô-la à sociedade. Trata-se de um modelo centralizado e redutor pelo qual uma classe superior determina como a classe inferior deve se comportar. O efeito das decisões da classe alta flui verticalmente para a vida das pessoas da classe baixa. O único perigo para um sistema piramidal é que os seres humanos agem em seu próprio interesse, e a lei legislada provavelmente reflete os interesses dos políticos, e não os das pessoas a quem é imposta. O sistema é uma fórmula para a corrupção e uma porta de entrada para o estado se expandir cada vez mais profundamente na sociedade.

Pode haver lei viável sem o Estado? Anarquistas e defensores do governo limitado têm debatido essa questão há séculos, com muitas vozes do livre mercado concluindo que a lei deve emanar do estado da mesma maneira que eles acreditam que o dinheiro deve. O direito é uma necessidade humana sem a qual a sociedade civil dificilmente durará muito. Se o livre mercado não pode fornecer esse bem essencial, então

o anarquismo falha e o governo limitado é a alternativa mais prática. A sociedade se tornará um parceiro júnior do estado. A eterna luta entre a Liberdade e o Poder sobre a qual Rothbard escreveu terminará com o Poder declarando vitória.

É uma abordagem útil começar definindo o termo "lei". Lei é um termo mais geral do que "legislação", que é meramente uma forma de lei; o termo geral refere-se a qualquer código ou conjunto de regras que governam a interação humana. "Governança" não implica em estado.

Pode haver lei sem um estado? A resposta: "sim, pode", e por um motivo: a sociedade precede o estado, que necessariamente surge da reunião de seres humanos que buscam interação. A sociedade precede tanto o estado quanto a lei.

Outra razão pela qual a lei de livre mercado pode existir é porque ela já existe.

Uma forma popular de lei de livre mercado é chamada de lei comum ou consuetudinária. Este é um conjunto de regras baseadas em precedentes que evoluem ao longo do tempo para resolver disputas em uma comunidade específica. Não é preventivo, mas reativo. Quando uma disputa irrompe, as partes vão a um terceiro imparcial ou a uma assembleia da comunidade para que seus casos sejam ouvidos. Em uma comunidade rural, por exemplo, se um homem acusa outro de roubar um animal de fazenda, então o árbitro avalia o caso e aplica um padrão comunitário que surgiu de casos semelhantes no passado. Uma vez que os próprios juízes podem estar envolvidos em uma futura disputa comunitária, eles têm interesse em infundir o processo com bom senso.

Isso é lei popular. É uma lei descentralizada que não tem a ampla aplicação das leis federais porque é adaptada às circunstâncias e padrões locais. Uma vila de pescadores quase certamente desenvolveria regras de comportamento diferentes de uma cidade de mineração, por exemplo. As regras que regem a comunidade de criptomoedas seriam diferentes das regras da indústria da construção. Enquanto o objetivo for preservar a interação pacífica e corrigir as violações, não há certo ou errado no conteúdo específico da lei.

O estudioso jurídico John Hasnas explica:

> O direito consuetudinário é o tipo de direito que evolui quando surgem disputas. […] Com o passar das décadas e séculos, à medida que as coisas evoluem, o tomador de decisões torna-se cada vez mais especializado, e quando você

> chega à era normanda na Inglaterra, as decisões são tomadas por júris. Os júris ainda são formados por pessoas comuns do país. […] Em nosso sistema, não se tem tribunais organizados de forma hierárquica até o final do século XIX, então já é 1873 e 1875.

Uma sociedade moderna complexa pode funcionar sem um conjunto homogeneizado de regras que são obrigatórias? A lei fundamentalmente descentralizada pode funcionar dentro de uma estrutura muito maior do que uma vila de pescadores ou uma comunidade rural?

A perspectiva tem sido discutida há séculos.

A Primeira Discussão da Lei de Livre Mercado e Sistemas de Defesa

> Ao nosso redor estão os benefícios quase inimagináveis de mercados, cooperação e tecnologia, mas de alguma forma somos ingênuos se não quisermos canalizar a atividade humana através das rampas de gado do governo. A vasta abundância material e digital que desfrutamos todos os dias é fornecida sem nenhum aparato estatal e, na verdade, o é *apesar* desse aparato. Este mundo privado não faz parte da realidade? O governo é o artifício, e os estatistas são os sonhadores utópicos que imaginam que indivíduos agindo sob a bandeira mágica do governo podem planejar, coagir e coordenar milhões de vidas.
> – Jeff Deist

O liberal clássico do século XIX Gustave de Molinari respeitava o livre mercado tão profundamente que seus colegas se referiam a ele como “a lei da oferta e da demanda transformada em homem”. Muito elogiado em sua época, Molinari caiu na obscuridade. Seu legado deve ser recuperado, no entanto, porque ele levantou uma questão crucial. Por que a segurança é um serviço monopolizado pelo estado e não executado pelo livre mercado, que fornece todos os outros serviços de forma mais eficiente e barata?

Molinari é o primeiro precursor explícito do anarquismo de livre mercado. Rothbard alude a seu ensaio de 1849, “Da produção de segurança”, como “a primeira apresentação em qualquer lugar da história

humana do que agora é chamado de 'anarcocapitalismo' ou 'anarquismo de livre mercado'". O núcleo do anarquismo de Molinari é sua teoria de como a sociedade surge.

> Há duas maneiras de considerar a sociedade. Segundo alguns, o desenvolvimento das associações humanas não está sujeito a leis providenciais e imutáveis. Em vez disso, essas associações, tendo sido originalmente organizadas de maneira puramente artificial por legisladores primitivos, podendo mais tarde ser modificadas ou refeitas por outros legisladores, de acordo com o progresso da *ciência social*. Nesse sistema, o governo desempenha um papel preeminente, pois é sobre ele, guardião do princípio da autoridade, que recai a tarefa cotidiana de modificar e refazer a sociedade.
> Segundo outros, ao contrário, a sociedade é um fato puramente natural. Como a terra em que está, a sociedade se move de acordo com leis gerais preexistentes. Nesse sistema, não existe, estritamente falando, ciência social; existe apenas a ciência econômica, que estuda o organismo natural da sociedade e mostra como esse organismo funciona.

Molinari acredita que os homens formam a sociedade por interesse próprio para satisfazer o mesmo "instinto de sociabilidade", demonstrado por outros animais de alta ordem; a sociabilidade foi construída na natureza do homem da mesma forma que a fome. A sociedade é organizada espontaneamente com o propósito de fazer trocas amplamente definidas; estas são a esfera apropriada do estudo econômico, não da ciência social.

Molinari apresenta três métodos pelos quais qualquer bem ou serviço pode ser produzido.

- O primeiro método é conceder um monopólio a uma entidade privilegiada. Isso é o que acontece quando o estado recebe o monopólio do uso da força e da lei dentro de uma jurisdição. Indivíduos dissidentes são forçados a obedecer, ou são silenciados.

- O segundo método é através de um coletivo que produz um serviço que diz beneficiar a sociedade em geral. A autoridade investida em uma democracia é um exemplo. Essa forma menos centralizada de controle não é menos perigosa para um dissidente.
- O terceiro método é a competição de livre mercado. A autoridade reside com indivíduos que são empresários e clientes. Os indivíduos escolhem livremente fazer negócios ou não.

Todos os serviços e bens devem ser questões puramente econômicas, incluindo segurança e defesa. Como todos os outros serviços que atendem a uma necessidade humana, a segurança é melhor fornecida por um livre mercado, no qual os indivíduos exercem o poder supremo do “sim” ou do “não”. Molinari é o primeiro teórico a apresentar um argumento coeso sobre como os mecanismos de livre mercado podem substituir as chamadas funções essenciais do estado, especialmente a proteção contra agressões. Ele afirma que o mercado também estabelece uma sociedade mais justa do que o governo.

> Essa opção que o consumidor retém de poder comprar segurança onde bem entender provoca uma constante emulação entre todos os produtores, cada produtor se esforçando para manter ou aumentar sua clientela com a atração do barateamento ou da justiça mais rápida, mais completa e melhor.
> Se, ao contrário, o consumidor não é livre para comprar títulos onde quiser, logo se abre uma grande profissão dedicada ao arbítrio e à má gestão. A justiça torna-se lenta e custosa, a polícia vexatória, a liberdade individual não é mais respeitada, o preço da segurança é inflacionado de forma abusiva e repartido de forma desigual, conforme o poder e a influência desta ou daquela classe de consumidores. Os protetores se envolvem em lutas amargas para arrancar clientes uns dos outros. Numa palavra, surgem todos os abusos inerentes ao monopólio ou ao comunismo.

Em suma, *não* deveria haver outra lei; que não a de livre mercado.

Molinari esboça brevemente um plano de como pode ser o serviço econômico de segurança. Para começar, ele se concentraria inteiramente na proteção da pessoa e da propriedade, em vez da proteção do estado ou de um código moral. Isso elimina a grande maioria das leis. Também reduz as guerras constantemente travadas por território por nações que desconsideram as preferências das populações.

A segurança seria um negócio – ou muitos negócios – incluindo forças policiais privadas e serviços de arbitragem. Os clientes em potencial provavelmente fariam uma série de perguntas a um provedor, incluindo uma que Molinari sugere; Será que "qualquer outro produtor de segurança, oferecendo garantias iguais … oferecerá … esta mercadoria em melhores condições?" Em suma, Molinari prevê um sistema de provedores de segurança que funciona da mesma maneira que as seguradoras de hoje. Ele conclui: "Sob um regime de liberdade, a organização natural da indústria de segurança não seria diferente da de outras indústrias".

Uma contrarresposta surge inevitavelmente; lei exige consenso.

Locke sobre o argumento do consenso para o direito

A percepção do problema da necessidade de consenso tem assombrado a questão do estado versus direito privado e justiça. Seu defensor mais persuasivo foi John Locke.

> A chave para… um sistema judicial anarcocapitalista é encontrada no conceito de um "judiciário pessoal". [Atuando como seu próprio juiz.] … O propósito dos tribunais é permitir que os homens resolvam disputas de modo a evitar a resolução violenta, bem como os ciclos de agressão-compensação. Considerar as decisões dos tribunais como legítimas é a única maneira de os litigantes evitarem ações *judiciais pessoais*.
> – Karl T. Fielding, "The Role of Personal Justice in Anarcho Capitalism" [ênfase adicionada]

"Judiciário pessoal" é uma ideia que Locke apresenta no *Segundo Tratado do Governo*. O termo refere-se ao direito natural de uma pessoa de avaliar suas próprias experiências e agir de acordo com suas conclusões; isso inclui julgar seu próprio caso. Além disso, como todos têm o

direito de reclamar sua propriedade de um ladrão, todos podem agir como seu próprio agente de restituição. Se alguém roubar sua carteira, você tem o direito de pegar o ladrão para recuperá-la. O agarrar é um ato de força defensiva, não de agressão.

Locke reconhece esse direito, mas acha insensato exercê-lo. Ele escreve:

> Que no estado de natureza cada um tem o poder executivo da lei de natureza, não duvido, mas será objetado que não é razoável que os homens sejam juízes em seus próprios casos, que o amor-próprio torne os homens parciais para si mesmos e seus amigos. E por outro lado, essa má natureza – paixão e vingança – os levará longe demais ao punir os outros; e, portanto, nada além de confusão e desordem se seguirão.

Não é sensato que os homens julguem seus próprios casos porque o ato produzirá conflito na sociedade. Mesmo um homem justo vê as coisas de sua própria perspectiva e interesse próprio; esta é a natureza humana. Além disso, ele pode se enganar sobre os fatos, inclusive fundamentais como a identidade do ladrão. Em outras palavras, mesmo um homem bom carece de objetividade. As pessoas que são menos honestas ou mais emocionais podem ser ainda menos justas e podem exigir remédios inapropriadamente severos.

Locke argumenta que uma sociedade na qual as pessoas julgam seus próprios casos cairá em "confusão e desordem". Por quê? Porque um veredicto injusto ou um remédio impróprio prejudica o destinatário que então julga *seu* próprio caso e retifica o malfeito a ele. O processo pode se tornar um ciclo sem fim porque a justiça administrada não é aceita como legítima por ambas as partes.

Locke acredita que quebrar o ciclo requer um juiz imparcial cuja avaliação seja amplamente aceita como legítima. Em termos de criptografia: Locke quer que a justiça descentralizada de cada homem julgando seu próprio caso seja centralizada e colocada sob a autoridade de uma terceira parte confiável. A necessidade de legitimidade na justiça é uma das principais razões pelas quais Locke defende um estado limitado. E, durante séculos, a abordagem de Locke tem sido usada para argumentar contra a possibilidade de direito privado e justiça na sociedade civil.

Mas se uma terceira parte confiável é irrelevante para exercer direitos como a liberdade de religião, ele não deveria ser verdade para o exercício de uma reivindicação de direito de propriedade sobre bens? Se a criptomoeda for roubada, a vítima não deveria poder recuperar sua propriedade diretamente hackeando as moedas?

Sim, diria Locke, mas há boas razões para não a exercer. Remédios individuais apresentam perigo para a vítima. Primeiro, se ele estiver enganado sobre a identidade do ladrão, o erro converte um ato de legítima defesa em uma agressão pela qual ele é responsável. Em segundo lugar, a vítima pode buscar mais remédios do que o apropriado, levando o agressor original a retaliar. Alcançar a restituição também pode ser perigoso ou além da capacidade da vítima. E assim por diante e assim por diante.

Julgar seu próprio caso também introduz o problema do bom samaritano. Os espectadores basearão seus julgamentos na aparência. Se eles testemunham um ataque na rua desde o início, eles sabem quem é o agressor, é claro. Sabem? E se você testemunhar um homem agarrar uma mulher e puxá-la rudemente para ele? Ela grita por socorro. Você corre para o resgate, atingindo o homem no rosto com um livro pesado que está carregando. Enquanto ele cobre o nariz quebrado, a mulher libertada sai correndo. Mais tarde você descobre que a mulher é uma batedora de carteiras; o homem estava recuperando uma carteira roubada.

Você facilitou um crime e feriu um homem inocente. E, no entanto, tudo o que você pretendia fazer era exercer um princípio corolário de autodefesa: o direito de defender pessoas inocentes contra agressões. Sem esse corolário, os cônjuges não poderiam se defender legitimamente e os pais não poderiam proteger os filhos. Você se comportou de maneira razoável, mas sua avaliação foi incorreta. O homem tinha o direito de cobrar remediação dela, e agora de você.

A confusão pode ser maior com o roubo de criptomoedas. Considere um cenário. Sua conta em uma corretora ou em seu disco rígido é limpa de moedas. Através do trabalho de detetive, você identifica o ladrão e busca a restituição invadindo sua carteira. Sua corretora detecta a atividade e vê *você* como o criminoso simplesmente porque é assim que aparece. A corretora chama a polícia e processa você. Eventualmente, você limpa seu nome à custa de dinheiro, inconveniência e constrangimento. Além disso, você não recupera as moedas.

Muitas vezes é impossível para um espectador distinguir entre uma vítima e um agressor através da observação. Isso é especialmente verdadeiro com crimes de criptomoedas. O homem que recupera sua carteira pode provar que é *sua* carteira mostrando o ID interno. Não é igualmente fácil provar que moedas ou dinheiro fiduciário pertencem a uma pessoa – uma moeda é uma moeda, um dólar é um dólar e eles não vêm com certificados de propriedade.

Felizmente, há uma maneira segura de identificar quem é a vítima.

O teste decisivo: quem é o proprietário do imóvel em questão? Ser proprietário significa ter um título válido para a propriedade. A posse pode até ser "9/10 da propriedade", mas o título é 100%. Ainda assim, a prova de título requer uma determinação baseada no exame das evidências.

> Se nenhum homem pode invadir a propriedade "justa" de outra pessoa, qual deve ser nosso critério de justiça? Não há espaço aqui para elaborar uma teoria da justiça nos títulos de propriedade. Basta dizer que o axioma básico da teoria política libertária sustenta que todo homem é dono de si mesmo, tendo jurisdição absoluta sobre seu próprio corpo. […] Segue-se então que cada pessoa é a justa proprietária de quaisquer recursos previamente não reclamados aos quais ela apropria ou mistura seu trabalho". A partir desses axiomas gêmeos – donidade de si mesmo e "apropriação original" – derivam a justificativa para todo o sistema de títulos de direitos de propriedade em uma sociedade de livre mercado. Este sistema estabelece o direito de cada homem à sua própria pessoa, o direito de doação, de legado (e, concomitantemente, o direito de receber o legado ou herança), e o direito de transferência contratual de títulos de propriedade.
> – Murray Rothbard

Como conceitos, roubo e restituição dependem da ideia de títulos de propriedade. Na maioria dos casos, a restituição é melhor feita por um agente ou agência terceirizada confiável. Contanto que o terceiro seja de livre mercado, isso apresenta poucos problemas. Ao contrário

da aplicação da lei, uma agência de livre mercado pode ser contratada e demitida à vontade. Essa é a diferença entre o Estado e a sociedade.

Antes de prosseguir para uma discussão mais concreta sobre segurança de livre e sua relevância para a criptomoeda, outro aspecto da segurança de livre mercado é melhor abordado: a prevenção do crime.

Segurança preventiva

> Talvez o principal problema nessa área seja ver a importância da proteção – fazer com que as pessoas se concentrem mais em deixar o criminoso fora e menos em prendê-lo depois que ele cometeu um crime. Esforços bem-sucedidos para reduzir a incidência de crimes devem ser baseados em melhores métodos de proteção. Ou seja, devemos nos preocupar em tentar prevenir as transgressões ao invés de nos preocuparmos com o que faremos depois que formos ofendidos. […] Os homens que veem a necessidade de proteção percebem que o governo não está em condições de fornecê-la, e eles dão as costas. A melhor fonte de proteção é o mercado.
> – Robert LeFevre, *The Fundamentals of Liberty*

Uma desvantagem de confiar sua segurança ao estado é a tendência de se tornar dependente dele e negligenciar a proteção a si mesmo. Se não houvesse polícia, as pessoas seriam mais agressivas em garantir preventivamente sua própria segurança. A situação se assemelha a como as pessoas abordam suas contas bancárias. Como a Federal Deposit Insurance Corporation assegura depósitos nos EUA contra falências bancárias, os clientes raramente pensam duas vezes na segurança de suas contas. Essa atitude ou hábito torna as pessoas vulneráveis a perder criptomoedas em corretoras ou investimentos imprudentes. A dependência do estado faz com que percam ou nunca desenvolvam o hábito da autoproteção. No entanto, a autoproteção é tanto responsabilidade do indivíduo quanto sua saúde.

LeFevre destaca outra desvantagem. Aqueles que utilizam os serviços de imposição da lei estão reforçando o mito da legitimidade do estado.

Então, como obter a justiça? LeFevre responde: defesas preventivas que evitam o crime antes que ele aconteça. Isso contrasta fortemente

com a forma como a maioria dos teóricos libertários aborda a justiça privada; eles se concentram quase inteiramente em questões como restituição versus retribuição. Essas questões entram em jogo, no entanto, somente após a ocorrência de uma violação de direitos. Como Satoshi, LeFevre quer um sistema que impeça que os crimes aconteçam em primeiro lugar.

Existem paralelos impressionantes entre LeFevre e Satoshi. Ambos querem evitar e substituir uma agência estatal terceirizada confiável por uma alternativa privada. LeFevre se concentra em substituir a aplicação da lei tradicional, enquanto Satoshi tem como alvo o sistema bancário central. Suas motivações são semelhantes. LeFevre vê a aplicação da lei como um fracasso maciço, ou muito pior. Sob o pretexto de fornecer justiça, oprime os indivíduos regulando quase todas as atividades deixando-os sem fôlego. Da mesma forma, Satoshi sabe que os bancos centrais e o dinheiro fiduciário são fracassos maciços, ou muito piores. Sob o pretexto de fornecer estabilidade e proteção financeira, eles saqueiam a riqueza dos indivíduos por meio de mecanismos como a inflação.

Ambos os homens não enfrentaram o estado, mas evitaram a necessidade dele. LeFevre escreve: “O governo é o único dispositivo que conhecemos de autoproteção? Não, não é. O seguro voluntário é outro dispositivo. Assim como policiais particulares, organizações privadas como a Legião Americana, vigias noturnos, polícia mercante, a Triple A e talvez uma dúzia de outros…”

As vantagens práticas aderem ao compromisso de LeFevre e Satoshi com a prevenção. Por um lado, após a ocorrência de um crime, pode ser quase impossível remediar a vítima, mesmo em casos não criminais de contrato ou atos ilícitos simples.

O estado não quer que as pessoas se protejam a si mesmas porque isso quebra seus monopólios de terceiras partes confiáveis sobre a aplicação da lei e os bancos. Ou, pelo menos, os ignora. O estado quer que as pessoas acreditem que a polícia “serve e protege”, porque então eles aceitam a perda da liberdade como o preço da segurança. A principal arma de autodefesa da sociedade é demonstrar que a proteção e os serviços do estado são desnecessários. As pessoas não precisam pagar com sua liberdade para estarem seguras

Uma Pergunta Assombrosa

A ênfase na prevenção captura um cisma dentro da comunidade cripto. Prevenção e desvio são companheiros naturais. O confronto não é. Qual abordagem é mais eficaz para lidar com o estado? Ou será que pode mesmo ser feita uma declaração geral? Satoshi parecia favorecer a ênfase na prevenção.

As duas atitudes estão incorporadas em um incidente entre Julian Assange e Satoshi. Ambos entendem completamente o valor da liberdade de cripto, mas parecem discordar sobre a melhor maneira de alcançá-lo.

Assange twittou em outubro de 2017: "Meus mais profundos agradecimentos ao governo dos EUA, senador McCain e senador Lieberman por pressionar Visa, MasterCad [sic], Paypal, AmEx, Moneybookers, e outros, a erguer um bloqueio bancário ilegal contra @WikiLeaks começando em 2010. Isso nos levou a investir em Bitcoin – com retornos > 50.000%.

A atitude de Satoshi é sintetizada por sua resposta a um tweet anterior de Assange que declara: "Pode vir [bitcoin]". Objetou Satoshi: "Não, não 'faça isso'. O projeto precisa crescer gradualmente para que o software possa ser fortalecido ao longo do caminho. Faço este apelo ao WikiLeaks para não tentar usar o Bitcoin. Bitcoin é uma pequena comunidade beta em sua infância." Menos de uma semana depois, em 12 de dezembro de 2010, Satoshi desapareceu após postar a mensagem: "WikiLeaks chutou o ninho de vespas, e o enxame está vindo em nossa direção". O enxame é o governo e, talvez, aqueles usuários que não se importam com o Bitcoin como veículo de liberdade e podem diluir seu potencial.

É tentador especular sobre o software com o qual Satoshi queria fortalecer o Bitcoin. Proteções contra maus agentes? Uma corretora descentralizada para negociação complexa e saque? É perturbador perceber que o Bitcoin pode ter sido prejudicado ao se popularizar cedo demais.

Mas a principal questão colocada aqui é se a atitude de prevenção e evasão de Satoshi é a abordagem mais eficaz para combater o estado. Nesse caso, aqueles que confrontam o estado com provocações e desafios podem estar enfraquecendo uma força primária da criptomoeda: liberdade por meio da prevenção, não do confronto. Eles podem estar devolvendo uma vantagem ao estado e afastando-a da sociedade. As teorias e estratégias de resistência não-violenta oferecem um plano de como lidar com o estado.

SEÇÃO CINCO

Cripto, Lei e Justiça

Lidando com o Crime sem o Estado

O desafio último para a cripto é o mesmo que confronta o próprio anarquismo: e enquanto a lei e a ordem? Como pode o crime ser prevenido e corrigido?

Os seres humanos precisam de justiça tão certamente quanto eles precisam de comida e abrigo. É um bem econômico que o livre mercado pode e irá satisfazer para lucrar. A dinâmica de como as criptos podem prevenir e corrigir o crime será amplamente tecnológica. Elas irão evoluir constantemente para atender às circunstâncias e preferências, a maioria das quais são imprevisíveis. O propósito aqui é esboçar os princípios e o contexto dentro do qual a justiça do livre mercado precisa funcionar e argumentar a favor de sua superioridade sobre o sistema estatal.

Comparado ao que?

A perfeição não existe. Ao avaliar e comparar sistemas que supostamente abordam o mesmo problema, pelo menos duas perguntas devem ser respondidas. Qual é o objetivo de cada sistema? E com que eficácia conseguem atingi-lo?

Apesar da palavra "justiça" aparecer em ambos os termos, os objetivos da justiça do livre mercado e da justiça do estado são incompatíveis. Uma empodera o indivíduo; a outra centraliza o poder nas mãos da autoridade. A justiça de livre mercado é a plena realização do direito de um indivíduo à autodefesa; a justiça estatal destrói o direito de autodefesa ao centralizá-lo nas mãos da autoridade. A situação é semelhante à do domínio financeiro. As criptomoedas e as blockchains permitem que os indivíduos se tornem self-bankers e controlem suas próprias finanças; moeda fiduciária e bancos centrais permitem que o estado monopolize as finanças e tire o controle das mãos dos indivíduos.

A metodologia e os objetivos dos dois sistemas são diametralmente opostos e, para compreendê-los, é útil compará-los especialmente no que diz respeito aos crimes cometidos por indivíduos uns contra os outros.

No entanto, deve-se primeiro declarar uma vantagem fundamental da justiça de livre mercado. A justiça de livre mercado aborda apenas o problema do crime – isto é, a violação de direitos – e atua apenas para

remediar as vítimas. O estado cria pseudocrimes – isto é, criminaliza o comportamento que é pacífico, porém "ofensivo" – e age apenas para proteger seu próprio poder. É difícil exagerar o impacto dessa diferença.

> O governo é uma fábrica de leis. Aprova leis da mesma maneira que uma fábrica produz e vende peças de metal [...], Mas, enquanto a fábrica está fornecendo um produto que é útil para os cidadãos em geral, e que os cidadãos que as comprarem o farão voluntariamente, a fábrica governamental fornece a coerção, que é útil principalmente para o próprio governo, e essa coerção é "comprada" [através de impostos e outras 'taxas'] antecipadamente pelo povo, que nunca está em posição de recusar a "compra".
> – Robert LeFevre, *The Nature of Man and It's Government*.

O sistema de justiça do estado fabrica rotineiramente dois tipos de criminosos reais – pessoas que violam intencionalmente os direitos dos outros. O maior grupo é formado por criminosos santificados que saqueiam riquezas e impõem o controle social em nome do estado. São políticos, burocratas, agentes da lei e outros agentes do estado ou seus comparsas. Quando as pessoas aceitam sua alegação de legitimidade e obedecem, eles governam com luvas de veludo. No entanto, quando as pessoas se recusam, a verdadeira natureza do sistema se revela e a obediência é comandada por meio da coerção crua: a violência.

O segundo grupo consiste em criminosos não santificados. São indivíduos que escolhem a violência ou a ameaça dela como um caminho rápido para o lucro, mas o fazem sem a pretensão de legitimidade. Criminosos comuns existiriam em qualquer sistema, mas a justiça estatal multiplica seu número oprimindo as pessoas de maneira a arrancar delas sua humanidade e a fazê-las abandonar toda crença na lei – qualquer lei. As prisões atuam como campos de treinamento para o crime; não apenas no sentido prático – o de como fazer –, mas também no sentido psicológico: o de por que fazer.

O sistema também produz pseudocriminosos – isto é, pessoas cujo comportamento é pacífico, porém "ofensivo", isto é: inaceitável para o estado. Traficantes e usuários de drogas são exemplos.

O estado se beneficia da fabricação de criminosos de pelo menos quatro maneiras:

- A necessidade humana de segurança e justiça dá ao estado uma justificativa para reivindicar o monopólio do uso da violência. O estado então centraliza e industrializa os “serviços” que fornece: a indústria legislativa, as burocracias regulatórias, a indústria policial, o sistema judiciário, a indústria prisional, o estado de vigilância e uma infinidade de outras indústrias associadas. O poder do estado está cimentado em todos os nichos da vida cotidiana.
- Se as pessoas acreditam que o estado é a única fonte de segurança, elas aceitam de bom grado a violência cometida por seus agentes. O povo presta obediência em troca de proteção, crendo não haver alternativa.
- O estado justifica impostos, multas e outras taxas em nome do financiamento da lei e da ordem. A “segurança” e todos os seus custos de fabricação, aplicação e manutenção são as gansas dos ovos de ouro dessa organização.
- Dinâmicas menos diretas, como o trabalho prisional, são extremamente lucrativas para o estado e para seus cúmplices corporativistas, que usam as prisões como centros fabris com mão de obra extraordinariamente barata.

Uma abordagem totalmente diferente é necessária para preencher a necessidade humana de segurança e justiça. Nada atende às necessidades humanas de forma tão eficiente e imparcial quanto o livre mercado. É necessário um retorno às raízes.

As apostas são altas. Reconsidere aquilo que atualmente dizem ser justiça.

O estado destrói o que não pode controlar

Comparar a justiça do livre mercado e a justiça estatal requer uma compreensão dos objetivos e da metodologia de cada uma. A justiça de livre mercado procura proteger a pessoa e a propriedade dos indivíduos e retificar qualquer violação com o mínimo de força possível. A justiça estatal busca manter o controle do estado sobre a sociedade e punir qualquer violação de suas regras com a força necessária para desencorajar novas violações. O objetivo do estado faz dele uma fábrica de leis; sua metodologia o torna uma fábrica de crimes.

> A maioria das pessoas não consegue avaliar os obstáculos fundamentais colocados no caminho da prevenção do crime pela lógica perversa da propriedade *pública*, da aplicação da lei *pública* e da prisão *pública*. Primeiro passo: comece com ruas públicas, calçadas e parques onde todos os cidadãos devem ter permissão de uso, a menos que se provem culpados de um crime. Etapa dois: apoie-se sobre uma burocracia pública inerentemente ineficiente para capturar, processar e julgar os criminosos contra os quais existem evidências suficientes de culpa. Terceiro passo: caso sejam condenados, sujeite os criminosos a um ambiente perigoso, improdutivo e, às vezes, incontrolável das prisões públicas para impedi-los de cometer futuras conduta antissociais. Etapa quatro: libere periodicamente a maioria dos prisioneiros de volta à sociedade e, depois, retorne à etapa um e repita o ciclo indefinidamente. Cada passo segue o passo anterior, e cada passo inevitavelmente deixa um espaço considerável para a conduta criminosa prosperar.
> – Randy Barnett, *The Structure of Liberty: Justice and the Rule of Law*.

Em suma, o estado cria criminosos não apenas por meio da legislação, mas também através de seu método de punição. Ele reivindica autoridade sobre o próprio cimento que as pessoas pisam, e depois as criminaliza por qualquer passo em falso. Isso não ajuda vítimas reais. Uma vez dentro do sistema de justiça, os criminosos têm pouca ou nenhuma chance de remediar seus erros por meio da restituição. Para a justiça estatal, a vítima geralmente é o próprio estado. Isso é especialmente verdadeiro para crimes sem vítimas – os chamados "crimes", nos quais todos os envolvidos, ironicamente, participam voluntariamente. Os crimes sem vítimas são responsáveis pela maioria das prisões.

O monopólio estatal da força é essencial para manter todos os outros monopólios, inclusive sobre o fluxo financeiro. Qualquer pessoa ou qualquer coisa que ameace esses monopólios é criminalizada, incluindo as criptomoedas. O estado identifica com precisão as criptomoedas como uma violação de seu monopólio e privilégios monetários. Isso significa que contornar o estado e os bancos centrais é criminalizado por estar associado à atividade do mercado negro e a outras condutas

pacíficas que privam o estado de receita. Esses pseudocrimes "justificam" a repressão estatal. Claro, as pessoas que usam dinheiro fazem o mesmo, mas há uma diferença notável na forma como o estado lida com crimes financeiros:

1. Os usuários-alvo são demonizados – profissionais do sexo, por exemplo – mas o dinheiro em si não é acusado de ser criminoso, talvez porque seja emitido por um agente do estado. Ou seja, a grande maioria das pessoas que usam dinheiro não são vistas como meliantes. Por outro lado, *tanto* os usuários *quanto* as criptos são demonizadas. A cripto é o verdadeiro alvo, com categorias de usuários que são vistas como desagradáveis sendo atacadas com destaque; uma tentativa de minar a legitimidade das criptomoedas.
2. Toda a categoria de usuários de criptomoedas é criminalizada – ou melhor, toda a categoria daqueles que usam criptomoedas *não regulamentadas*. Esta é uma característica da justiça estatal. Categorias de pessoas se tornam criminosas – traficantes de drogas e profissionais do sexo, por exemplo – independentemente de algum deles ter agredido outro indivíduo. Novamente, o dinheiro está isento desse tratamento, com a grande maioria dos que usam o dinheiro estatal não sendo acusados de crime.

O problema fundamental do estado com as criptomoedas, em oposição ao dinheiro, é que as criptomoedas tornam possível confiar em estranhos. Isso faz do próprio estado um estranho, porque ele é sempre o último a ser confiável. Se os indivíduos não exigirem os serviços do estado, não haverá razão legítima para ele existir. É por isso que o estado está tão desesperado para convencer as pessoas de que elas precisam dele para ter dinheiro, segurança, aposentadoria, assistência médica, educação e todos os outros bens do livre mercado e todos os outros serviços que puderem requisitar. O atual sistema de justiça não trata da proteção da sociedade ou dos indivíduos, mas da preservação do estado.

Infelizmente, uma segunda justificativa apoia a campanha do estado contra as criptomoedas não regulamentadas: a alegação de que as criptomoedas violam os direitos individuais. Especificamente, diz-se que as criptomoedas estão envolvidas em violência contra indivíduos, como o tráfico humano. O aspecto "infeliz" dessa justificativa é que algumas acusações são verdadeiras. Este é o ataque mais perigoso do estado às criptomoedas, porque dá a entender que pessoas decentes que

ficam e devem ficar horrorizadas com crimes como o tráfico humano simpatizam com ele.

Um artigo do bitcoin.com de março de 2018 aborda outro crime real: fraude. “Todos os dias são perdidos cerca de $9 milhões em golpes de criptomoedas.”

> No tempo que você leva para ler esta frase, $850 terão sido perdidos em golpes de criptomoeda. No tempo necessário para concluir este artigo, esse valor terá subido para $17.000. Phishing; fraude; roubo; hacking; e os números são sempre altos. Nos primeiros dois meses de 2018, ocorreram 22 golpes separados envolvendo roubos de $400.000 ou mais. Junte todos os números e isso equivale a uma média de $9,1 milhões por dia. Ah, e isso não inclui os valores discrepantes de 2018 – Coincheck, Bitconnect e Bitgrail. Caso contrário, o total seria de $23 milhões por dia.

O estado usa crimes reais como cobertura para atingir seu verdadeiro objetivo em relação à cripto: eliminar a concorrência que ameaça um de seus monopólios vitais: o dinheiro. Parte da campanha do estado é exagerar os crimes reais, e com isso apresentar seu serviço como o único remédio possível.

As criptomoedas são acusadas de proteger quase todos os atos de violência concebíveis. O artigo “10 das maiores mentiras contadas sobre o Bitcoin” trata da acusação de que as criptomoedas são o dinheiro preferido do terrorismo.

> Se você quer culpar uma moeda, tente o dólar americano, que tem sido usado para financiar mais guerras, guerras por procuração, bombardeios, sequestros e insurgências do que qualquer outra moeda. A Europol não encontrou evidências de que terroristas estivessem usando criptomoedas para financiar suas atividades. Isso não quer dizer que já não tenha acontecido ou que não vá acontecer. É revelador, no entanto, que as únicas pessoas que ligam o bitcoin ao terrorismo são os governos, que buscam reprimir as moedas digitais.

As criptos também são acusadas de facilitar grupos de ódio.

> Poderíamos lançar uma longa explicação sobre o porquê de ser ridículo culpar uma moeda pelas ações de um pequeno subconjunto de seus usuários, mas às vezes as respostas mais simples são as melhores: "Você provavelmente já ouviu falar sobre carros – mas o que você certamente não ouviu é o quanto eles estão ajudando os ladrões de banco."

Muitas vezes é difícil enxergar através da fumaça, discernir os crimes frios e cruéis nos quais as criptomoedas estão envolvidas das próprias criptomoedas. Mesmo assim, esses crimes devem ser combatidos. E não apenas porque convidam ao envolvimento do Estado, mas também porque as vítimas merecem reparação. No entanto, concordar com o Estado neste ponto é o início de uma disputa mais profunda que se resume a questões mais fundamentais.

O que é Justiça?

> O libertarianismo é sobre direitos individuais, direitos de propriedade, livre mercado, capitalismo, justiça ou o princípio de não agressão. Ainda assim, nenhuma dessas coisas é suficiente para explicá-lo completamente. O capitalismo e o livre mercado descrevem as condições catalácticas que surgem ou são permitidas em uma sociedade libertária, mas não abrangem outros aspectos do libertarianismo. E direitos individuais, justiça e agressão resultam em direitos de propriedade, pois, como Murray Rothbard explicou, direitos individuais são direitos de propriedade. E a justiça é apenas dar a alguém o que lhe é devido, e isso depende de quais são seus direitos.
> – Stephan Kinsella, "What Libertarianism Is."

O que é justiça? A resposta é: a estrutura rudimentar de qualquer sistema de direito. O filósofo político americano Michael Sandel responde: "A maneira mais simples de entender a justiça é dar às pessoas o que elas merecem. Essa ideia remonta a Aristóteles. A verdadeira dificuldade começa com descobrir *quem* merece *o quê* e *o porquê*". [Ênfase adicionada] Isso é justiça privada. Ela precisa de mais definição.

A justiça privada é distinta da justiça divina, mas às vezes as duas se confundem. A justiça divina supõe uma deidade ou algum outro poder supremo responsável e capaz de pesar o valor de cada pessoa em uma balança, aplicando ao réu o destino que a deidade julgar como justo. "Por que eu, ó Senhor, por que eu?" é o grito de quem acredita ter sido traído pela justiça divina. A teoria por trás desse "grito de socorro" é que há algo, além da não agressão contra sua propriedade, que uma boa pessoa tem o direito de exigir do mundo: boa saúde, por exemplo. Quando coisas ruins acontecem, a situação é chamada de "injusta". Porém, a palavra está sendo usada coloquialmente ou sendo mal utilizada. Talvez uma palavra melhor seria "azar".

A justiça privada não é baseada em uma divindade ou algum outro poder transcendente. É, como sustenta Aristóteles, justiça que consiste nas pessoas receberem o que merecem umas das outras. E, como Kinsella explica na primeira citação: "justiça é apenas dar a alguém o que lhe é devido, e isso depende de quais são seus direitos". Baseia-se na natureza humana e na autopropriedade de cada indivíduo.

O conteúdo da justiça privada baseia-se em dois princípios. A primeira é a não iniciação da força, que é uma reafirmação do dever de uma pessoa de respeitar a autopropriedade dos outros; a justiça reside em viver juntos em paz. O segundo princípio é o direito contratual, pelo qual uma pessoa troca voluntariamente com outra. A justiça aqui reside em cada pessoa recebendo o que foi acordado. Quando a justiça não ocorre, é necessário um remédio. No entanto, nem uma quebra de contrato nem seu remédio precisam envolver violência. Uma violação nem sequer precisa ser culpa de uma pessoa; poderia ser ocasionada por qualquer outra coisa, como uma mudança inesperada das circunstâncias. Mesmo assim, a pessoa prejudicada pela violação ainda tem o direito de ser remediada.

É aí que começa e termina o direito à justiça. Porém, há uma confusão comum sobre justiça. Nominalmente, muitas vezes é chamado de "injusto" quando uma parte trata a outra com desrespeito ou hostilidade. Isso pressupõe que uma pessoa possa ter, numa situação dessas, o direito à reivindicação de reparação pela atitude da outra pessoa. Mas, esse direito não existe; há apenas o direito de viver sem ser agredido ou ameaçado e ao cumprimento de um contrato. É improvável que um vendedor que seja rude com um comprador tenha negócios repetidos, e isso é um forte incentivo para que ele seja civilizado. Mas o único dever do vendedor sob a justiça é ser não violento e ser honesto na troca; ser

agradável, embora favorável a ambas as partes, é totalmente opcional. Como Rothbard escreve: “Não é função da lei tornar alguém bom, reverente, moral, educado ou gentil”.

Voltando à declaração inicial de Sandel, o *quem* da justiça é duplo: 1) quem é privado do que é seu por direito – autonomia corporal, propriedade ou um benefício contratado, 2) e quem é responsável por fornecer reparação à vítima. O *como* é abordado neste capítulo. O *porquê* é por conta do fato de cada pessoa ser um proprietário de si mesmo.

Poucas coisas são tão justas quanto o livre mercado, em que duas pessoas trocam diretamente por valores acordados e depois vão embora, cada uma satisfeita. Uma mulher que compra um tomate e vai para casa com sua compra para fazer uma salada está aproveitando a justiça. O vendedor de tomates que embolsa o dinheiro da mulher e passa para o próximo cliente também está experenciando a justiça. Assim, o livre mercado oferece às pessoas o que elas merecem por direito. Em outras palavras: o livre mercado é a justiça aristotélica na prática.

Outra maneira de dizer isso é que a justiça privada é proprietária. Em seu ensaio “A Teoria Proprietária da Justiça na Tradição Libertária”, o cofundador do Movimento Voluntarista Moderno, Carl Watner, fornece um resumo justo da justiça privada: “A teoria proprietária da justiça está preocupada com apenas uma coisa: a determinação crucial de títulos de propriedade justos versus títulos de propriedade injustos de indivíduos em relação a seus próprios corpos e aos objetos materiais ao seu redor.”

O teórico mais persuasivo da justiça proprietária pode muito bem ser o jurista libertário Randy Barnett. Em seu livro *The Structure of Liberty*, Barnett argumenta que a lei deve ser administrada de forma privada, com quaisquer ineficiências deixadas sob a responsabilidade do livre mercado. Parte da eficiência da justiça proprietária deriva de sua pura simplicidade e do número mínimo de leis. Barnett escreve sobre o sistema atual: “Cada dólar gasto para punir um usuário ou vendedor de drogas é um dólar que não pode ser gasto cobrando restituição de um ladrão. Cada hora gasta investigando um usuário ou vendedor de drogas é uma hora que poderia ter sido usada para encontrar uma criança desaparecida. Todo julgamento realizado para processar um usuário ou vendedor de drogas é tempo de tribunal que pode ser usado para processar um estuprador”. Barnett argumenta que o direito privado é a solução para a corrupção inevitável que surge dos interesses adquiridos e dos monopólios.

Os Requisitos do Direito de Contratos Privados

O direito contratual exige apenas duas coisas para funcionar: a presença de um acordo e um instrumento de execução. O contrato é a presença do acordo; expressa o consentimento e os termos de aceitação. Os contratos podem ser implícitos, verbais ou escritos, mas quanto mais explícito for o acordo mais fácil será a administração da justiça.

O obstáculo sobre o qual a lei muitas vezes tropeça é o instrumento de execução. Como você aplica a lei em outra pessoa e executa restituição? Surgem daí questões éticas e práticas. Uma questão ética comum: e os direitos individuais daqueles forçados a fornecer restituição? Uma resposta comum: quem viola os direitos de outro renuncia aos seus na proporção do dano infligido e até que esse dano seja remediado. Uma questão prática comum: a restituição convida à participação de uma terceira parte confiável. Na lei estatal, a terceira parte é composta por agentes do estado, que costumam usar a violência. No direito proprietário ou de livre mercado o terceiro consiste em agentes do livre mercado, que são restringidos por dinâmicas como o uso da força proporcional e a necessidade de preservar uma boa reputação. Mas qualquer modelo que dependa de uma terceira parte confiável é vulnerável à corrupção, incompetência e outros riscos.

Satoshi removeu das trocas econômicas o problema das terceiras partes confiáveis, e a blockchain também pode removê-lo de muitas áreas da lei. Uma transferência peer-to-peer na blockchain atende a todos os requisitos de um bom contrato. Ela incorpora um acordo voluntário; memoriza os termos da troca; sua validade é comprovada pela transparência. A blockchain também pode cumprir um dos requisitos da lei – ou seja, é um instrumento de execução por si só. Quando isso acontece, é chamado de contrato inteligente – um contrato autoexecutável. Um relatório recente do Senado dos EUA afirma: “O conceito [de contratos inteligentes] está enraizado no direito básico dos contratos. Normalmente, o sistema judicial julga disputas contratuais e impõe termos. Com os contratos inteligentes, um programa impõe o contrato embutido no próprio código.” Os contratos inteligentes oferecem a mesma oportunidade de evitar terceiras partes confiáveis de advogados e tribunais do estado, assim como as criptomoedas evitam os bancos centrais. Além disso, ao atuar como o acordo e o instrumento de execução, a

criptomoeda pode eliminar grande parte das despesas dos serviços de justiça.

Os contratos inteligentes de hoje são, sem dúvida, primitivos em comparação aos que virão, mas também são uma prova de que a ideia funciona.

O impacto na sociedade causado pela tecnologia dos contratos autoexecutáveis pode ser enorme. Em uma sociedade organizada em torno da troca, os contratos seriam a base de *toda* lei. Até o uso da violência, que viola os direitos individuais, pode ser visto como uma violação do dever – o contrato implícito – de que todos devem respeitar os direitos dos outros se quiserem reivindicar esses direitos para si. Mais uma vez, aqueles que cometem crimes perdem seus próprios direitos na mesma medida em que os negaram a outrem e enquanto o erro não for sanado, isto é: enquanto a vítima não for remediada. Em seguida, o contrato é restabelecido. Toda lei pode ser reduzida ao contrato.

Um artigo no *Futurism*, "Um escritório de advocacia de IA quer automatizar todo o mundo jurídico", indica o quão fácil pode ser a transição de contratos físicos e advogados para contratos inteligentes e algoritmos. "No LawGeex [um serviço automatizado], os usuários carregam um contrato e, em um curto período (uma hora, em média), recebem um relatório informando quais cláusulas não atendem aos padrões legais comuns. O relatório também detalha quaisquer cláusulas vitais que possam estar faltando e onde cláusulas existentes podem exigir revisão. Tudo isso é calculado por algoritmos." Por uma taxa modesta, a LawGeex pode detectar cláusulas que permitem fraudes ou fornecem proteção inadequada.

Esses serviços destacam um aspecto raramente discutido da justiça: o fato de que ela é um serviço. Basicamente, há dois aspectos da justiça proprietária: Os proprietários devem pagar o custo de proteger sua propriedade, se assim o desejarem e os criminosos devem pagar todos os custos da restituição, que incluem a própria restituição, as despesas para obter a remediação e a inconveniência ou sofrimento da vítima.

> "A análise econômica do crime começa com uma simples suposição: os criminosos são racionais. Um assaltante é um assaltante […] porque essa profissão o torna melhor, segundo seus próprios padrões, do que qualquer outra alter-

> nativa disponível para ele [...] Se os assaltantes são racionais, não temos que tornar o assalto impossível para evitá-lo, apenas inútil ... Se velhinhas começarem a carregar pistolas em suas bolsas, de modo que um assalto em dez coloca o assaltante no hospital ou no necrotério, o número de assaltantes diminuirá drasticamente – não porque todos tenham sido baleados, mas porque a maioria terá mudado para formas mais seguras de ganhar a vida. Se o assalto se tornar suficientemente não lucrativo, ninguém o fará".
> – David Friedman, *Rational Criminals and Profit-Maximizing Police*.

Qualquer um que valorize sua propriedade deve tornar os crimes contra ela não lucrativos e difíceis. Essa abordagem por si só poderia reduzir em muito os crimes. No entanto, as pessoas geralmente lidam com sua segurança pessoal de uma dessas quatro formas:

- Elas se auto protegem, assumindo diretamente a responsabilidade por sua própria segurança e pela de sua propriedade. Isso envolve custos como fechaduras, prática de autodefesa e, portanto, um certo investimento de tempo.
- As pessoas ignoram sua própria segurança, confiando na sorte ou na boa vontade dos outros. O custo é o dano potencial à sua propriedade e à sua pessoa.
- As pessoas confiam na proteção do estado. O custo é a sua liberdade e a chance de segurança real.
- As pessoas veem a segurança como um serviço privado ao qual assinam – contratar um vigia noturno, por exemplo. O custo é o custo do serviço.

Se segurança é um bem econômico, como comida ou abrigo, então o consumidor do bem deve arcar com o preço de adquiri-lo, e o custo nem sempre é monetário. O preço a se pagar pode muito bem ser o tempo e a energia necessários para configurar proteções. (Veja a discussão sobre proteção no capítulo anterior).

Um vislumbre de como a proteção do livre mercado pode funcionar para as comunidades são as redes de confiança (networks), que não contam com a proteção da polícia, e que ainda assim precisam cuidar e

cuidam de si mesmas. Considere as profissionais do sexo. A propriedade a ser protegida, nesse caso, é o próprio corpo da profissional do sexo.

Em seu artigo "Cem anos de anarquia criptográfica", a engenheira Blockchain Elaine Ou comenta: "A encriptação de chave pública não serve apenas para encriptar mensagens privadas. Ela também fornece provas de que o remetente é quem diz ser. Quando compradores e vendedores realizam transações, eles assinam mensagens com suas chaves privadas. As assinaturas se tornam identificadores digitais." Se isso parece muito distante da prevenção à violência, converse com profissionais do sexo, cuja principal forma de defesa é verificar as identidades e reputações dos clientes, que elas compartilham umas com as outras por meio de redes de confiança (networks). Uma das responsabilidades menosprezadas de um cafetão – muitos dos quais não são abusivos – é garantir a segurança das profissionais do sexo, seja examinando clientes, manuseando dinheiro, fornecendo transporte ou lugares seguros e esperando. Os cafetões são terceiras partes confiáveis, mas como quaisquer terceiros, podem trazer mais problemas do que soluções. A criptografia muda essa dinâmica para que algumas tarefas de um cafetão sejam substituídas por um filtro peer-to-peer com transparência. Assim, a profissional do sexo está no controle, e isso se traduz em menos risco de violência e mais dinheiro, o que promove a segurança.

O segundo aspecto da justiça proprietária é a necessidade de obrigar os criminosos a pagarem o preço de remediação de suas vítimas. Mas como isso poderia se dar?

Um mecanismo de restituição comumente proposto tem sido a agência de defesa privada (PDA). O PDA é um negócio de livre mercado cujos lucros e a reputação dependem da precisão e justiça de suas práticas na remediação do crime. Uma vítima de crime escolhe livremente sua terceira parte confiável, cuja confiança é testada pela presença constante de concorrentes. A relação comercial dura apenas enquanto o cliente valoriza o serviço.

O objetivo do PDA é recuperar das mãos do criminoso os bens roubados ou danificados, ou no mínimo o valor deles; novamente, a propriedade danificada pode ser o corpo da vítima. Mas o PDA também atua como proteção para a vítima e para o próprio agressor durante o processo de remediação. A vítima é protegida de qualquer dano ou perigo que possa estar envolvido; o agressor lida com um profissional que deseja apenas garantir a remediação, e não a dar vazão à raiva da vítima,

de quaisquer outros ou de sua própria. De fato, o PDA tem um forte incentivo comercial para evitar as despesas e complicações de ferir alguém.

Friedman oferece uma visão de um PDA em seu livro *Machinery of Freedom*. De início, o autor considera "o caso mais fácil" de um conflito, que é "a resolução de disputas envolvendo contratos entre firmas bem estabelecidas [...]. Um desenvolvimento recente; historicamente, a aplicação veio do desejo de uma empresa de manter sua reputação".

Mas e as disputas envolvendo violência, incluindo roubo? "A proteção contra a coerção é um serviço", explica Friedman. "Atualmente, é vendido em uma variedade de formas, como guardas da Brinks, fechaduras, alarmes contra roubo etc. À medida que a eficácia da polícia estatal diminui, esses substitutos de mercado para a polícia, como os substitutos de mercado para os tribunais (os contratos inteligentes), tornam-se mais populares. Suponha então que em algum momento futuro não haja polícia estatal, mas sim agências de proteção privada. Essas agências vendem o serviço de proteção a seus clientes. Talvez eles também garantam desempenho ao segurar seus clientes contra perdas resultantes de atos criminosos". O seguro que foi adquirido de um PDA torna-se a solução imediata oferecida à vítima, talvez da mesma maneira que o seguro de carro paga por danos após um acidente; o PDA pode então buscar a solução do criminoso com o bônus de adquirir seu lucro. Ou a vítima pode contratar o PDA após o crime ter sido cometido, e então o PDA investigaria e recuperaria tanto a propriedade quanto o custo de seus serviços diretamente do agressor.

Friedman conclui: "O que descrevi é um arranjo muito improvisado. Na prática, uma vez que as instituições anarcocapitalistas estiverem bem estabelecidas, as agências de proteção antecipariam tais dificuldades e providenciariam contratos com antecedência, antes mesmo que os conflitos específicos ocorressem [...]" Mas, novamente, não é possível prever futuros mecanismos de restituição.

Na verdade, a resposta mais precisa para uma pergunta feita anteriormente – como seria a justiça proprietária? – é uma que muitas pessoas acharão insatisfatória. Ninguém sabe, assim como ninguém sabia como o Bitcoin se formaria e como se manifestaria.

A razão pela qual a aparência futura da justiça proprietária é imprevisível

Na obra *Human Action,* de Ludwig von Mises, onde o autor defende o conceito de "consumidor soberano", que expressa como consumidores e produtores se relacionam em uma economia de mercado. Os produtores são o motor da prosperidade, afirma Mises, mas não são eles que determinam a direção que uma economia toma. Esse poder pertence aos consumidores. Mais especificamente à preferência dos consumidores. Essas preferências diversas levam a uma explosão de escolhas econômicas – uma dinâmica que seria verdadeira para os serviços de segurança e justiça.

A soberania do consumidor vai contra a crença dominante de que são os capitalistas e os grandes empresários que determinam o curso de uma economia, assim como a vida das pessoas, que participam dela. É aquela velha ideia tradicional: a de que o controle econômico está nas mãos de quem tem a propriedade dos meios de produção, enquanto as pessoas comuns são forçadas a aceitar as migalhas.

Para Mises, a relação é simbiótica, sendo o consumidor um parceiro igual ou maior. Ele descreve a soberania do consumidor:

> A direção de todos os assuntos econômicos é, na sociedade de mercado, uma tarefa dos empresários; deles é o controle da produção. Eles estão no leme e dirigem o navio. Um observador superficial acreditaria que eles são supremos. Mas eles não são. Os empresários, ao contrário do que se pode pensar, são obrigados a obedecer incondicionalmente às ordens do capitão, e o capitão é o consumidor. Nem os empresários, nem os agricultores, nem os capitalistas determinam o que deve ser produzido. Apenas os consumidores têm o poder de fazer isso. Se um empresário não obedecer estritamente às ordens do público que lhe são transmitidas pela estrutura de preços de mercado, ele sofre perdas, vai à falência e, assim, é afastado de sua posição no leme. Outros que se saírem melhor em satisfazer a demanda dos consumidores o substituirão.

Uma consequência da soberania do consumidor é que ninguém pode prever as preferências expressas no mercado, incluindo os próprios consumidores. Ninguém pode prever as instituições, agências ou dinâmicas que surgirão para lucrar com essas preferências. Sem dúvida,

a tecnologia e outras inovações evoluirão para oferecer novas alternativas; a mudança será vertiginosa. Mises observa:

> "Eles [os consumidores] não são chefes fáceis. Estão sempre cheios de caprichos e fantasias, mutáveis e imprevisíveis. E não se importam nem um pouco com o mérito passado. Assim que lhes é oferecido algo que eles gostam mais ou é mais barato, os consumidores abandonam seus antigos fornecedores."

O livre mercado muda constantemente em resposta à forma como os consumidores votam com seu dinheiro. É fluido, constante e está além da capacidade de previsão de qualquer pessoa. A soberania do consumidor é uma das principais razões pelas quais não é possível oferecer um plano fixo de como a justiça proprietária funcionará no futuro. Só é possível descrever os conceitos que cercam a justiça, mas não suas aplicações específicas.

Rumo a uma nova visão de justiça

As criptomoedas mudaram a visão do mundo sobre o dinheiro – do que era e do que poderia ser… Ou será. A justiça proprietária também revoluciona o conceito e a aplicação da lei. Em ambos os casos, os princípios e definições permanecem inalterados. O dinheiro é um meio de troca, uma forma de riqueza e uma unidade financeira. Justiça é cada um receber o que merece; a lei é o meio e as regras de execução da justiça. Mas a forma que a justiça proprietária assume, como as criptomoedas, é algo novo sob o sol.

Tradicionalmente, o estado justifica seu monopólio sobre o dinheiro e a justiça apontando para uma suposta necessidade de "consenso". O estado justifica seu monopólio monetário pela chamada necessidade de que uma moeda seja "confiável" e amplamente aceita em um determinado território. Lockeanos justificam o próprio estado pela suposta necessidade da sociedade civil de um árbitro final de justiça cujo julgamento seja "confiável" e geralmente aceito dentro de um determinado território. (O consenso que é compelido pela força, é claro, não é consenso; indica o contrário.)

O consenso é o raciocínio do século passado. É inválido para a moeda; é inválido para a justiça. As criptomoedas provaram que o consentimento individual, junto com um instrumento de aplicação – a blockchain –, cria uma moeda válida. Não importa se os usuários individuais constituem uma pequena parcela da população. Como na América colonial, uma infinidade de moedas pode circular para preencher uma variedade de nichos e preferências. E o mesmo acontece com a justiça.

As pessoas que estabelecem contratos entre si podem ter uma visão de justiça diferente da de seus vizinhos ou do público em geral. A primazia dos contratos e o uso da blockchain significam que, desde que a violência seja evitada, não há uma justiça universal. O que for acordado é justo. Quem acredita que cobrar juros é errado, por exemplo, fará empréstimos que não incluem nenhum. Para os capitalistas, o oposto será verdadeiro. Ambos os arranjos são justos, com o conteúdo da justiça sendo definido pelos seus participantes.

O ponto mais importante: os indivíduos contratantes definirão seu próprio padrão de justiça, que pode e irá variar de contrato para contrato dentro da mesma jurisdição. Isso separa a justiça da geografia – dos ditames de uma autoridade que reivindica jurisdição sobre um determinado território – e localiza o conteúdo da justiça dentro dos próprios indivíduos. A justiça é descentralizada até o nível máximo: o do indivíduo.

O estado recorre ao argumento do consenso porque sua jurisdição está inerentemente ligada à geografia. Uma nação é definida geograficamente e um estado é a instituição que reivindica jurisdição sobre uma nação específica, a qual ele tenta manter sob controle através do monopólio do uso legítimo da força. Na realidade, o consenso que o estado alega ter advém de sua própria autoridade, que todos dentro da jurisdição são compelidos, sob ameaça, a honrar. A população deve aceitar a moeda legal, obedecer à lei e obedecer às vontades e aos decretos de seus juízes; ninguém está autorizado a discordar. Ninguém.

Mas o que acontece quando a geografia se torna irrelevante para a lei e a justiça como a transferência de dinheiro é agora? Nesse caso, o estado ainda seria capaz de exercer sua “autoridade”?

As criptomoedas respondem esta pergunta: Cruzando o globo como o vento e não assumindo qualquer nacionalidade, as criptomoedas sobrevoam pontos físicos de engarrafamento, chamados bancos, assim como linhas imaginárias, chamadas fronteiras. A cripto ignora a geografia, assim como ignora o problema das terceiras partes confiáveis. O

estado perde o monopólio do dinheiro e do sistema financeiro, que é sua força vital. Quando a geografia se torna irrelevante, o estado também se torna, pois o estado é uma reivindicação territorial, e as criptomoedas tratam essa questão de maneira peculiar: elas não dão a mínima.

Esta é a Justiça sem fronteiras geográficas. Esta é a justiça das criptos. A justiça que não passa pelo engarrafamento da lei estatal, que impõe aceitação às normas do estado. Essa é a justiça descentralizada, a que expressa apenas as preferências dos indivíduos envolvidos. Essa noção de justiça visa libertar os indivíduos da "justiça" estatal da mesma maneira que as criptomoedas os libertaram do dinheiro fiduciário monopolizado pelo estado.

Infelizmente, a necessidade percebida de consenso faz com que as pessoas acreditem que a justiça de livre mercado é "anárquica" no pior sentido da palavra. Elas não entendem os princípios, o propósito e conteúdo da justiça proprietária. Seu princípio central é o direito de cada indivíduo de viver em paz. Seu propósito é facilitar as trocas voluntárias entre os indivíduos para que cada um receba o que merece; quando não o fazem, então o propósito se torna a restituição. Exceto pela proibição da violência, o conteúdo da justiça seria tão variado quanto as próprias criptomoedas, porque os indivíduos decidiriam o que é exatamente da mesma maneira que decidem o preço adequado de um bem – por meio de um acordo.

Declarado de outra forma: A blockchain atua como o contrato, a lei e o mecanismo de aplicação em um único pacote. Ela incorpora os termos com os quais as partes concordaram, aplica esses termos sem o envolvimento de terceiros e garante que sua aplicação ocorra sem considerar jurisdições geográficas. Assim como a cripto evita o monopólio monetário, a justiça blockchain pode contornar os monopólios de aplicação da lei e justiça do estado.

A confusão das pessoas sobre a lei e a justiça de livre mercado é compreensível porque os conceitos vão contra tudo o que os foi ensinado. O que aprenderam é incorreto; não apenas a teoria, mas também a história.

Em seu artigo, "Por que as Elites Preferem um Sistema Legal Centralizado", o historiador Chris Calton explica como a visão convencional de justiça centralizada foi incorporada. "A motivação para centralizar a autoridade legal foi inteiramente política." Uma função vital da sociedade civil foi usurpada e homogeneizada em nome da consistência e do consenso. Isto nem sempre foi desse jeito. Calton continua:

> "Mas no início do século XIX, a consistência era menos valorizada do que a flexibilidade no sistema jurídico. Quando os tribunais eram locais, as pessoas de uma determinada comunidade tinham interesse em que a justiça fosse feita de acordo com as particularidades de cada caso individual. [...] E para aqueles que não tiveram a sorte de se encontrar no topo da hierarquia jurídica – os sem instrução, os pobres, as mulheres, as crianças e os negros – essa flexibilidade sustentava até mesmo as noções modernas de justiça – ainda que imperfeitamente – com mais eficácia do que os tribunais centralizados e legalmente consistentes que se seguiram."

A lei foi descentralizada para o nível local, a fim de atender às necessidades da população local. E se a lei centralizada nem sempre existiu, então ela não é inevitável nem necessária. O passo final, é claro, é descentralizar a justiça para o indivíduo.

Na verdade, instâncias de lei descentralizada funcionam ao nosso redor agora e oferecem modelos práticos para a construção de novos sistemas. Uma delas é chamada Creative Commons Law (CCL). A CCL é um empreendimento de código aberto para construir um sistema jurídico prático para sociedades sem estado. Ela enfatiza a aplicação concreta e de forma alguma bloqueia outros sistemas concorrentes. A maioria das pessoas encontrou uma manifestação do CCL: as licenças Creative Commons para publicação de material têm sido tradicionalmente vistas como o limite da propriedade intelectual, dos direitos autorais e patentes.

Muitos autores e inventores descartam a legitimidade da PI e oferecem seu trabalho sem as restrições normais de direitos autorais na republicação; outras licenças Creative Commons especificam termos como creditar a fonte original na reimpressão. O autor ou inventor escolhe a licença que prefere; sua escolha de forma alguma infringe as pessoas que escolhem diferentes termos de publicação, como os que buscam preservar um quase monopólio de seu trabalho. Ideias e desenvolvimento de código aberto têm sido a base da comunidade de cripto. A CCL é uma prova da lei de livre mercado.

Em resumo, a justiça da blockchain é uma justiça proprietária, que está livre das jurisdições geográficas conhecidas como nações. Ela

é limitada, em vez disso, por algoritmos e escolhas. Não requer consenso ou o envolvimento da terceira parte confiável chamado estado. O código é a lei, e o conteúdo do código é o que os envolvidos concordam. Os indivíduos definem e executam sua própria lei sem uma legislatura ou um processo político. E, se a justiça consiste em cada pessoa receber o que merece – isto é, receber a troca acordada – então cada indivíduo também define a justiça para si mesmo. A única restrição é a de que os acordos devem ser voluntários; ou seja, de que eles devem ser o que são: acordos.

> "O anarquismo e a liberdade não dizem nada sobre como as pessoas livres se comportarão ou sobre quais arranjos escolherão. Simplesmente diz que as pessoas têm a capacidade de escolher os arranjos que farão e quais os que não farão. O anarquismo não é normativo, ele não diz como se deve ser livre, mas apenas que a liberdade pode existir."
> – Karl Hess, "Anarchism Without Hyphens".

Sem a necessidade de consenso, várias versões da lei e da justiça podem e irão coexistir pacificamente dentro de um território. Elas podem funcionar diretamente ao lado um do outro ou dentro da mesma casa, e podem variar de contrato para contrato para a mesma pessoa, dependendo de seu propósito e de suas circunstâncias. Se alguém prefere a lei comum ocidental enquanto um vizinho judeu prefere a lei hassídica, que assim seja; ninguém está vinculado aos valores do outro, porque a execução de termos de uma pessoa de forma alguma impede a capacidade do outro de executar um conjunto diferente de termos. Os comunistas podem rejeitar uma cláusula politicamente censurável, como pagar aluguel, enquanto os capitalistas podem exigir que os contratos a incluam.

O código é a lei. A execução do código é justiça. Os indivíduos estão no controle.

Considere a dinâmica de um crime específico: A Fraude

O crime ainda existiria sob a justiça blockchain, pois sempre existirá em todas as sociedades, mas seria reduzido ao mínimo.

Um dos crimes privados contra os quais os usuários de criptomoedas exigem mais proteção é a fraude, que é uma forma de roubo. Certamente não é o único crime, mas examinar a fraude pode fornecer informações sobre como os outros podem ser tratados.

Roubo é a usurpação de propriedade sem o consentimento do proprietário; ou seja, nenhuma transferência de título acompanha a transferência real de um bem. Onde quer que a propriedade termine, o título permanece com o proprietário. Se a propriedade foi tomada por meio de violência direta, como num roubo, então ocorreu um assalto. Se foi obtida por meio de engano, o roubo é chamado de fraude. A fraude pode consistir em uma falsa troca de valor; uma pessoa vende um Rolex que é, na verdade, uma imitação barata, por exemplo. Ou a troca pode ocorrer em termos falsos; o Rolex genuíno acaba por ser uma propriedade roubada, sobre a qual o vendedor não tem nenhum título e nenhum direito de propriedade. O vendedor mente; o comprador acredita; o contrato de venda – explícito ou implícito – é inválido, pois a troca acordada não ocorreu. Não houve troca, apenas fraude.

Antes de discutir a fraude cripto, no entanto, é importante perceber que o crime pode não ser tão comum quanto muitos supõem.

A Australian Competition & Consumer Commission divulgou um relatório sobre o nível e os tipos de golpes que aconteceram em 2017. Fraudes relacionadas às criptomoedas constituíram 0,6% do total. Ou, como uma manchete da Panda Security afirmou recentemente:
“A fraude com criptomoedas é a exceção, não a regra.”

Para cada golpe, existem milhões de oportunidades que são criadas pela criptografia e pela blockchain para aumentar a riqueza e facilitar a cooperação entre os usuários. No entanto, cada caso de fraude chama mais atenção do que merece, porque as acusações são usadas para exigir regulamentação. Para exigir o envolvimento do estado.

Prestar atenção à fraude é necessário, é claro, mas o problema requer mais do que atenção. Requer uma diligência por parte dos usuários, que não pode ser legislada. Veja o golpe “mybtgwallet.com”, em 2017: O mybtgwallet.com ofereceu aos usuários carteiras Bitcoin Gold online gratuitas, através das quais eles poderiam verificar seus saldos e realizar transações gratuitas por um tempo limitado. A carteira era uma fraude, mas ganhou credibilidade ao aparecer brevemente no site oficial do Bitcoin Gold – um ato de extremo descuido, na melhor das hipóteses, por parte deste site. Para aceitar a oferta do mybtgwallet.com, os usuários precisavam enviar suas chaves privadas ou chaves de recuperação.

Um link fraudulento era um aspecto oculto do processo. Depois que usuários desavisados aceitaram a oferta da mybtgwallet, a criptomoeda em suas carteiras foi encaminhada para outros endereços: os endereços dos criminosos. De acordo com a Coindesk, "num elaborado esquema, mais de $3,3 milhões foram roubados de usuários de bitcoin, que buscavam reivindicar sua parte da criptomoeda recém-criada: a Bitcoin Gold. Pelo menos $30.000 em Ethereum, $72.000 em Litecoin, $107.000 em Bitcoin Gold e mais de $3 milhões em Bitcoin foram furtados."

Ninguém deveria ter caído nesse golpe porque ninguém deveria ter entregue suas chaves privadas, mas mesmo os veteranos das criptomoedas o fizeram. O fato de terem feito isso não significa que "eles mereciam"; esta não é a mensagem aqui. Uma pessoa com dinheiro transbordando de seus bolsos pode decidir dormir em um beco atrás do bar. Sua escolha é tola e perigosa, mas não o torna legalmente responsável se o dinheiro for roubado. Ela seria, ainda assim, vítima de um crime. Infelizmente, aqueles que entregam chaves privadas a estranhos fazem o equivalente a dormir em um beco com bolsos salientes. Essas pessoas seriam aconselhadas a desenvolver hábitos de advertência. Parte da propriedade em um mundo predatório é descentralizar a autodefesa, incluindo a defesa da propriedade.

Quais são algumas das lições a se aprender com o desastre do mybtgwallet.com para evitar fraudes? As especificidades incluem:

- Sempre assuma que um site estranho pode estar tentando roubar suas criptomoedas, sua identidade, seus dados ou todos esses itens. Estenda a confiança real somente após tomar as devidas precauções.
- Não lide com sites que exijam algo além das informações pessoais mais básicas. Prefira aqueles que incentivam o pseudonimato.
- Amigo ou não, nunca confie a ninguém seus dados privados ou suas chaves de recuperação. Isso equivale a divulgar a combinação de um cofre ou entregar um maço de dinheiro para alguém segurar enquanto você faz uma ligação. Dados e chaves de recuperação são a prova e o controle de propriedade. Eles constituem o título de propriedade da cripto.
- Nunca guarde seus dados ou chaves em qualquer lugar que seja vulnerável a ser copiado por outra pessoa.

- Sempre mantenha uma versão em papel de ambos em um local seguro como backup.
- Em essência, mantenha a privacidade. Os ladrões precisam de acesso para saquear. Não deixe suas portas abertas.

Essas são as especificidades. Mas esse é o ponto mais geral e fundamental: sempre tome as devidas precauções e sempre proteja a sua propriedade. Essas são as responsabilidades que advém da propriedade para o proprietário; as responsabilidades dos dados e dos usuários. Lembre-se: quando a criptomoeda sai de uma carteira, ela desaparece para sempre. Pelo menos essa deveria ser a sua suposição. A transação não pode ser revertida e poucas corretoras ou outros ramos da cripto oferecem seguro contra roubo. Até mesmo vítimas determinadas com casos documentados raramente recebem de volta mais do que alguns centavos de dólar, como as vítimas da Mt. Gox fizeram após anos e anos de exaustivo esforço.

Felizmente, a situação está mudando devido à necessidade de proteção do mercado. Um artigo de junho de 2019 no Zero Hedge comentou: “Os preços das criptomoedas foram atingidos da noite para o dia depois que a Binance, a maior corretora de criptomoedas do mundo, sediada em Hong Kong, revelou que hackers haviam fugido com 7.000 bitcoins – no valor de aproximadamente $41 milhões a preços atuais – roubados da ‘hot wallet’ da corretora. No entanto, os preços rapidamente reduziram algumas de suas perdas depois que a corretora anunciou que os clientes não seriam responsáveis pelas perdas: em vez disso, os depositantes seriam remediados com ativos da ‘Secure Asset Fund for Users’ da Binance.” E assim, a SAFU foi criada em 3 de julho de 2018, como uma resposta do mercado ao desejo de segurança dos usuários. A Binance aloca 10% do valor das taxas de trading realizadas em seu site e as transfere para um fundo de armazenamento em uma carteira fria para proteger os clientes em “casos extremos”.

Mecanismos de mercado e educação financeira minimizam os danos e eventos de fraude, possibilitando que pessoas desafortunadas ou descuidadas sejam protegidas. No entanto, é difícil proteger aqueles que correm para as criptomoedas por conta de FOMO (Fear Of Missing Out, medo de estar perdendo algo), assim como é difícil proteger aqueles que entregam suas economias nas mãos de estranhos contra o roubo. O crime sempre ocorrerá; o objetivo é reduzi-lo ao mínimo.

Quando a fraude ocorre, as pessoas clamam por regulamentação do governo. Mas há uma ironia sutil e amarga nessa dinâmica. Uma das razões pela qual as pessoas podem ser propensas à fraude é porque elas abordam a riqueza e os investimentos com uma mentalidade estatista. Ou seja: elas estão acostumadas às garantias de segurança do estado. Essas garantias são ilusões, mas isso não importa; o que importa para influenciar o comportamento das pessoas é que elas acreditem nas garantias. Nos EUA, por exemplo, a Federal Deposit Insurance Corporation garante o dinheiro que uma pessoa deposita em um banco até o valor de $250.000. A aplicação da lei opera divisões de fraude que registram relatórios do crime. Em suma, o estado faz com que as pessoas se sintam mais seguras do que deveriam, e isso as faz negligenciar as devidas precauções. O estado induz as pessoas a renunciar seu senso de responsabilidade.

A terceira parte confiável mais fraudulenta do mundo – o estado – não é um remédio. Suas falsas garantias vêm ao custo de sacrificar a privacidade e a liberdade individual, que são as maiores precauções de todas as riquezas. E, no fim, a riqueza ainda é saqueada.

Uma Revolução Prática e Descentralizada

A Revolução Satoshi está aqui e agora. É uma revolução prática, que é descentralizada ao nível individual.

Primeiro, a parte prática: a perfeição não é possível quando administrada por seres imperfeitos. Os criptoanarquistas que criaram o Bitcoin não eram apenas idealistas, mas também realistas; eles sabiam que o mundo e as criptomoedas nunca estariam perfeitamente a salvo da violência. O estado se intrometeria e as carteiras seriam hackeadas. Eles também sabiam que trabalhar em direção a um ideal é a única maneira de chegar o mais próximo possível dele. A situação é semelhante à ingestão diária de vitaminas: embora a saúde perfeita possa não ser alcançada, vitaminas e exercícios levarão alguém o mais próximo possível disso. E aproximar-se de ideais como a justiça é uma jornada que vale a pena, mesmo que o destino nunca seja alcançado.

O idealismo prático tem pelo menos dois benefícios utilitários. A rede de princípios para uma sociedade ideal é um mapa intelectual para avaliar se um ato específico se aproxima ou se afasta da liberdade. Se a liberdade de expressão é um dos princípios, por exemplo, suprimir um livro ofensivo afasta-se da liberdade e não deve ocorrer. Um ideal é

como o verdadeiro Norte em uma bússola. Ele diz: “Sim, esta é a direção correta”. A única coisa mais poderosa do que uma ideia cuja hora chegou é um *ideal* cuja hora chegou.

A descentralização: A Revolução Satoshi é uma revolução das expectativas crescentes; ela é impulsionada pelo desejo de liberdade, privacidade financeira e esperança para o futuro. A revolução está ocorrendo em uma base individual, porque não é mais necessário que as pessoas se levantem em massa, concordem com estratégias revolucionárias ou coordenem eventos por meio de comitês de terceiras partes confiáveis. Cada usuário se rebela sem drama ou ideologia enquanto persegue o interesse próprio, que é a motivação humana mais forte de todas. O interesse próprio em *todas* as suas formas deve ser a base de uma revolução bem-sucedida. Qualquer um que permaneça fiel à visão de Satoshi acerca das criptomoedas se manterá, quer queira ou não, como um lutador da liberdade, porque a descentralização radical do poder é a definição da Revolução, da nossa Revolução: da Revolução Satoshi.

O estado continua sendo o maior criminoso de todos; seu poder não deve ser subestimado, mas também não deve ser temido. A melhor atitude e abordagem em relação ao estado que já vi foi a do falecido Samuel E. Konkin III (SEK3), o pai do Agorismo e um velho companheiro de bebida. SEK3 atendia rotineiramente seu telefone com a saudação “Smash the State”; sua atitude em relação ao estado era infalivelmente rebelde. E, no entanto, sua atitude não era a abordagem prática que adotava em relação ao estado. Seu estilo de vida não enfatizava confrontos diretos com a autoridade; desafiar era sua atitude, não seu estilo de vida. Sempre que possível, SEK3 evitou contato e substituiu quaisquer serviços valiosos que o estado usurpou do livre mercado – como os bancos – com os privados. Suas ações eram um plano ambulante sobre como derrotar o estado eliminando-o de sua vida, porque ele sabia que a maneira mais eficaz de esmagar o estado era estabelecer alternativas privadas para torná-lo irrelevante, ou seja: privar o estado de sua vida privada.

O legado duradouro da SEK3 para a teoria anarquista foi o sistema econômico-filosófico chamado Agorismo, que busca uma revolução pacífica por meio da contra economia. SEK3 o definiu como “o estudo e prática de toda ação humana pacífica que é proibida pelo estado”. A contra economia é a versão “mercado negro” da praxeologia

de Mises, a qual Mises define como "o estudo da ação humana". O sistema de SEK3 é o estudo da ação humana necessária para negar a presença do estado na vida pessoal e na sociedade. Esmague o estado em atitude, substituindo-o na vida cotidiana. Não "esmague [literalmente] o estado"; apenas contorne-o.

SEK3 teria se deleitado com a audácia da criptomoeda que foi criada com a atitude "Smash the State", mas que adota a abordagem de evitar o confronto direto. Ele teria reconhecido imediatamente que estabelecer uma moeda melhor e de livre mercado é a maneira mais segura de enfraquecer a moeda fiduciária. Ele teria, com a mais absoluta certeza, declarado a criptomoeda "a moeda contra econômica" – a moeda do Agorismo. Mas mais do que isso. Em um piscar de olhos, o SEK3 teria reconhecido as implicações das criptomoedas para a justiça – exatamente porque elas evitam e substituem as leis estatais pelas do livre mercado, da privacidade e dos contratos. Em minha mente, consigo ver meu amigo Samuel tomando um gole da cerveja preta horrível que ele adora, seguido por uma tragada em seu cachimbo constantemente presente, antes de anunciar: "A anarquia chegou!"

Posfácio

Eu pretendia terminar este livro discutindo o impacto da blockchain na violência física, nos crimes de violência. Eu não posso. Não acho que haja impacto. Não sei como a blockchain poderia impedir estupros em becos, por exemplo. Eu poderia falar sobre colocar o trabalho sexual em um registro financeiro aberto, mas isso seria um chá fraco, e pareceria uma evasão. Este é um livro de teoria original, que explora o que nunca foi dito antes sobre criptomoedas. Nem sempre sei para onde as ideias estão me levando, mas o impacto na violência física não é um desses destinos.

E é por isso que estou, agora mesmo, escrevendo o posfácio do meu livro.

Minha jornada pelas criptomoedas começou em uma cozinha no Chile. Fui a palestrante de destaque em uma conferência, que também apresentou um painel de três outros especialistas em Bitcoin. Meu marido e eu decidimos alugar uma casa pelo AirBnb porque queríamos estender aqueles dois dias em duas semanas de saltos pelo país, o que foi mágico. A casa em que acabamos, no entanto, foi equipada para casamentos. Tradução: Havia cerca de trinta camas amontoadas em aproximadamente vinte quartos, que eram ligados por pisos feitos de compensado rachado, abaixo dos quais havia um desnível de dois andares. Não era uma casa; era uma aventura … com um banheiro funcionando. Eu prefiro chamá-la de exótica.

A conferência abrigou os palestrantes e atendentes em um complexo remoto, que rapidamente se encheu. Os organizadores nos pediram para receber os especialistas em Bitcoin. Nós concordamos com prazer. Eram sujeitos agradáveis e apresentáveis – embora homens que falavam de assuntos que não faziam sentido para mim. Felizmente, meu marido desenvolve hardware e software para sistemas embarcados, então estou acostumada a nem sempre entender as coisas.

E então houve a manhã depois que eles chegaram. Um sujeito dormiu até tarde. Um insistiu em preparar o café da manhã; não pretendo caluniá-lo, porque ele era muito agradável e tentava ser um bom hóspede. Mas as pessoas não cozinham perto de mim. Eu cozinho; você come; nos damos bem. Ele cozinhou…

Então, eu estava de mau humor quando olhei do outro lado da mesa do café da manhã para os olhos negros como carvão de Michael Goldstein, que mais tarde descobri ser fundador do Instituto Satoshi. Um jovem notável. Michael é apelidado de Bitstein por quem tem carinho por ele… e, sendo sincera, tudo que você precisa fazer é conhecê-lo para que isso aconteça. Quando olhei em seus olhos, tive uma sensação familiar, porque tenho espelhos no meu próprio banheiro. “Ele é um fanático”, concluí. Acontece que gosto de fanáticos, dependendo do tópico em discussão, é claro. E eu não tinha nada contra as criptomoedas, que começaram a me interessar porque as pessoas que eu admirava as levavam muito a sério.

Com um olhar inabalável, Bitstein me disse que a blockchain era um registro financeiro aberto que daria luz à anarquia. Ok. Eu imediatamente entendi o poder da cripto para contornar o sistema bancário central… *se* fosse amplamente adotado; *se* não fosse proibido, *se*, Mas por que anarquia?

Todas as minhas ressalvas eram políticas e totalmente diferentes das de meu marido, que se juntou a nós depois de cerca de quinze minutos. Brad esperou até que Michael respirasse fundo e então disse uma palavra: “escalabilidade”. Foi a primeira vez que Michael tropeçou. Ele disse: “estamos trabalhando nisso”. Eu vi Brad perder algum interesse.

Mas eu não. Eu não sabia o que escalabilidade significava nesse contexto, exceto no senso comum. Mas eu não me importei porque a palavra “anarquia” tinha sido pronunciada, e isso eu sabia. Michael parecia mais do que feliz em abandonar a escalabilidade para a política, e eu investiguei por que ele achava que o alvorecer da liberdade havia chegado como uma cavalaria em um algoritmo.

Michael respondeu, e não me convenceu, mas me instigou a ler. Assim como meu velho amigo Jeff Tucker. Assim como o incrível Stephan Kinsella. Outras pessoas tentaram aumentar minha consciência também. Mihai Alisie, da *Bitcoin Magazine*, me pediu para escrever para ele sobre o anarquismo, por exemplo. Acho que não agradeci adequadamente a ele por ter tanta confiança em mim. E naquele ponto, sua confiança provavelmente era infundada. Enviei um artigo para a Bitcoin Magazine, que estava longe de ser o meu melhor trabalho. Isso atraiu uma resposta melhor do que eu merecia: eles estavam dispostos a “trabalhar comigo”. Agradeci ao editor e recuei com a desculpa absolutamente genuína de que não sabia se tinha algo original para contribuir para a discussão. Eu não tinha nada de novo para dizer. Eu ainda não

tinha entendido as arestas duras e frias da teoria cripto e não entendia seu poder. O que significava que eu ainda não tinha demarcado a única área onde eu poderia e posso contribuir com algo original: a integração do criptoanarquismo com a rica história da teoria anarquista-libertária que se estende por séculos.

À medida que lia mais, fiquei envergonhada de mim mesma. Criptoanarquismo: o desenvolvimento político mais importante da minha vida ocorreu sem que eu percebesse, o que é imperdoável. Eu havia gastado meu tempo com o libertarianismo "oficial" – institutos orientados por doações e definidos por doações, universidades financiadas por impostos, revistas acadêmicas. Quando foi que a liberdade chegou embalada em dólares de impostos, prêmios e homenagens entregues em jantares beneficentes? A liberdade é uma luta de rua. O criptoanarquismo tomou as ruas sem que eu percebesse. Mas agora eu o vejo.

Roger Ver. Nosso primeiro contato foi um e-mail que ele enviou do nada. O e-mail de Roger me conquistou de primeira, porque ele usou a palavra "voluntarismo". Em 1982, fui uma das três pessoas que criaram o movimento voluntarista moderno durante uma conversa fiada, em um apartamento de dois quartos com aluguel recente em Hollywood, Califórnia. Lembro-me de meus dedos literalmente zumbindo com a excitação das ideias e planos que estávamos forjando na época: Carl Watner, George H. Smith e eu. Mas, principalmente, Carl. Era e é quase inacreditável para mim que, décadas e décadas depois, um visionário voluntarista chamado Roger estivesse batendo à minha porta (por assim dizer). Ele me pediu para escrever para seu site.

Roger teve um bom timing. Em linguagem de ficção científica, eu finalmente *grokkei* (entendi) o bitcoin; Além disso, tiro meu chapéu para Robert A. Heinlein por inventar essa palavra. E tiro meu chapéu para Roger e toda a equipe do bitcoin.com por nunca – e quero dizer, nem uma vez, de qualquer maneira – terem tentado influenciar minhas ideias enquanto eu as desenvolvia nas minhas tentativas (às vezes desajeitadas) de integrar o criptoanarquismo nas tradições mais amplas do liberalismo clássico, da economia austríaca e do anarquismo individualista.

A montagem do livro se transformou em uma reescrita maciça, seguida por um período de edição feroz. O livro diante de você agora é baseado nas colunas que eu serializei no bitcoin.com, mas pelo menos metade do material é novo – especialmente a seção sobre justiça.

Antes de encerrar, devo abordar outro aspecto do criptoanarquismo. Eu não esperava esse efeito colateral benéfico, mas aí está ele; a vida é muitas vezes inesperada. O mundo cripto me fez jovem novamente.

Tive a imensa sorte de fazer amizade e passar muitos anos com pessoas que ajudaram a fundar o movimento libertário. Murray Rothbard costumava brincar, nas conferências de 1980, dizendo que o libertarianismo poderia ser eliminado por uma bomba bem colocada. Ele estava certo, mas agora o movimento é imenso. Vão precisar de uma bomba maior.

Ainda assim, há uma desvantagem para toda essa minha sorte: as pessoas com quem cresci na intelectualidade adulta agora me fazem sentir velha, principalmente porque muitas delas estão mortas; eu geralmente era a mais nova na sala. Sentir-se velho é sentir-se cansado, sem nada à vista que faça seus olhos brilharem.

Lembro-me de Murray e de sua paixão– lembro-me tão vividamente …, Mas, ao longo dos anos, algo deu errado com sua paixão. Veio da raiva, eu acho, e se expressou atacando outras pessoas. Lembro-me de um jantar pós-conferência em que um colega teve a infelicidade de dizer algo positivo sobre Keynes. E então – Deus nos ajude! – ele elaborou. Murray finalmente explodiu em um discurso retórico com sua voz chiada broklinesca, e o sujeito começou a recuar. Acho que ele teria empurrado sua cadeira para fora do restaurante, se essa fosse uma possibilidade. O colega admitiu que Keynes podia estar errado sobre "esta" questão, e sobre "aquela" questão. E que, provavelmente, Keynes poderia ser considerado "fraco" no contexto histórico. Murray desceu a mão aberta sobre a mesa e disse em voz alta: "E Hitler foi 'fraco' com os judeus!". Todos rimos, embora sabendo que aquilo havia sido um ataque… e um aviso.

A cripto brilha como uma coisa girando ao sol; e o brilho é limpo, porque não vem da raiva ou de humilhação de alguém ou qualquer coisa parecida. A paixão que vem dela é positiva. Uma porta se abriu, e não sei onde o caminho que ela mostra me levará, porque nunca poderia ter previsto até onde cheguei. Que os tijolos amarelos sejam gentis comigo.

Uma coisa eu sei: estou em boa companhia; a crew do bitcoin.com não foi nada menos que decente e sorridente para essa mulher que ousou se intrometer em seu mundo. Isso significa muito para mim. Não sei onde vou parar em seguida, mas sei que a tecnologia – e não apenas as criptos – vai nos dar uma aventura selvagem pelo resto de nossas vidas.

Minhas mãos estarão sobre o teclado, dedicadas a colocar as mudanças corriqueiras em perspectiva histórica, mesmo enquanto elas estiverem acontecendo.

Eu tenho uma chance de fazer isso … porque eu sou jovem novamente; estou esperançosa. E nada, nada é impossível. Foi isso que este livro significou para mim. Faço uma pausa nesta jornada, neste exato momento, para te agradecer por fazer parte dela:

Seja bem-vindo à Revolução Satoshi.

FERNANDO **ULRICH**

BITCOIN

A MOEDA NA ERA DIGITAL

Prefácio de Jeffrey Tucker

Fernando Ulrich

BITCOIN
A MOEDA NA ERA DIGITAL

1ª Edição

Mises Brasil

2014

Título
BITCOIN - A MOEDA NA ERA DIGITAL

Autor
Fernando Ulrich

Esta obra foi editada por:
Instituto Ludwig Von Mises Brasil
Rua Iguatemi, 448, conj. 405 – Itaim Bibi
São Paulo – SP
Tel: (11) 3704-3782

Impresso no Brasil / *Printed in Brazil*

ISBN: 978-85-8119-078-5

1ª Edição

Revisão
Leandro Augusto Gomes Roque
Fernando Fiori Chiocca

Revisão Final
Alexandre Guaspari Barreto

Capa
Neuen Design

Projeto gráfico
Estúdio Zebra
Ficha Catalográfica elaborada pelo bibliotecário
Pedro Anizio Gomes– CRB/8 – 8846

U45b ULRICH, Fernando
Bitcoin: a moeda na era digital / Fernando Ulrich. -- São Paulo : Instituto Ludwig von Mises Brasil, 2014.
100p.

1. Moeda 2. Tecnologia 3. Sistema Monetário
4. Liberdade 5. Dinheiro I. Título.

CDD – 332.4:004.678

Índice para catálogo sistemático:

1. Dinheiro – 332.4
2. Tecnologia (internet) – 004.678

Sumário

Agradecimentos

Primeiramente, agradeço aos irmãos Fernando e Roberto Fiori Chiocca pela ideia deste livro e pela confiança em mim depositada como encarregado da realização deste projeto. Sem esse estímulo inicial, talvez esta obra jamais tivesse sido escrita. Agradeço ao Instituto Ludwig von Mises Brasil (IMB) pela publicação e ao Helio Beltrão, presidente do IMB, pelo convite para fazer parte dessa nobre instituição e pelo apoio a mim sempre dispensado, especialmente em relação a esta iniciativa.

Pela cuidadosa e rigorosa revisão, agradeço ao Leandro Roque, editor do IMB, e, novamente, ao Fernando Fiori Chiocca. Pela revisão final, sempre precisa e meticulosa, agradeço ao Alexandre Barreto. Agradeço também ao Jerry Brito e à Andrea Castillo pela permissão para traduzir parte de sua obra aqui reproduzida no segundo capítulo.

Não posso deixar de mencionar dois brilhantes economistas por desbravar o estudo econômico aplicado ao Bitcoin de forma formidável e original, Konrad S. Graf e Peter Šurda. Agradeço também ao Jeffrey Tucker pelo belo prefácio e pela sua sempre contagiante defesa da liberdade.

Por fim, agradeço à minha família pelo carinho e suporte constante durante a realização deste livro, em especial, à minha esposa, Karine, pela paciência inesgotável, pela energia sempre positiva e pelo incentivo fundamental para a conclusão desta obra.

Ao Joaquim, que a sua geração colha os frutos de uma moeda honesta

Bitcoin, a nova moeda internacional

por Jeffrey Tucker

POR MUITOS SÉCULOS, A MOEDA EM CADA PAÍS era distintos nomes para essencialmente a mesma coisa: uma commodity, geralmente ouro ou prata. Estes eram o que o mercado havia selecionado pelas suas propriedades únicas particularmente adequadas à função monetária. Esse universalismo da moeda serviu bem ao mundo porque promovia o livre-comércio, auxiliando os comerciantes no cálculo econômico, e provia um freio sólido e confiável ao poder dos governos. Ela limitava o impulso nacionalista.

Duas formas de nacionalismo arruinaram o sistema monetário antigo. Os próprios estados-nação descobriram que o melhor meio para o aumento do poder se dava pela depreciação do dinheiro, o que acaba sendo menos doloroso e mais opaco do que o método tradicional de tributar a população. Para escaparem imunes desse processo, governos promoviam zonas cambiais, protecionismo e controle de capitais, removendo, assim, um elemento do crescente universalismo do mundo antigo.

Então, no início do século XX, os governos nacionalizaram a própria moeda, removendo-a do setor das forças competitivas de mercado. O banco central foi, nesse sentido, uma forma de socialismo, mas de uma variedade especial. Governos seriam o arbitrador final no destino do dinheiro, mas a sua gestão diária seria tarefa do cartel dos bancos com a garantia de proteção contra a falência – à custa da população.

O novo poder de criação de moeda sob o regime de bancos centrais foi imediatamente posto em prática por meio das mortes em massa da Primeira Guerra Mundial. Foi uma guerra total e absoluta – a primeira guerra internacional da história que fez de toda a população parte do esforço de guerra – e financiada por endividamento lastreado no novo poder mágico dos governos de usar o sistema bancário para fabricar receita com a impressora de dinheiro.

Oposição intelectual a essas políticas nefastas emergiram durante o período entreguerras. Os economistas austríacos lideraram a batalha em direção à reforma. A não ser que alguma coisa fosse feita para desnacionalizar e privatizar o dinheiro, alertaram eles, o resultado seria uma série infinita de ciclos econômicos, guerras, inflações catastróficas, e a contínua ascensão do estado leviatã. A suas previsões foram assustadoras e precisas, mas não são motivo de satisfação, pois foram impotentes para impedir o inevitável. No decorrer do século, a maior parte dos bens e serviços da sociedade estava melhorando em qualidade, mas a moeda, agora removida das forças de mercado, apenas piorava. Tornou-se o catalizador do despotismo.

Durante todas essas décadas, lidar com esse problema foi algo que intrigou os economistas. A moeda precisava ser reformada. Mas o governo e os cartéis bancários não tinham nenhum interesse nessa empreitada. Eles beneficiavam-se desse sistema ruim. Centenas de livros e conferências foram realizados incitando uma restauração do universalismo do mundo antigo do padrão-ouro. Os governos, porém, os ignoraram. O impasse tornou-se particularmente intenso depois de os últimos vestígios do padrão-ouro serem eliminados na década de 70. Mentes brilhantes tinham prateleiras repletas de planos de reforma, mas eles acumularam nada além de pó.

Tal era a situação até 2008, quando então Satoshi Nakamoto tomou a iniciativa incrível de

reinventar a moeda na forma de código de computador. O resultado foi o Bitcoin, introduzido ao mundo na forma menos promissora possível. Nakamoto lançou-o com um white paper em um fórum aberto: aqui está uma nova moeda e um sistema de pagamento. Usem se quiserem.

Agora, para sermos justos, já haviam ocorrido tentativas prévias de projetar tal sistema, mas todas falharam por uma das duas razões: 1) eram usualmente detidas de forma proprietária por uma empresa comercial e, portanto, apresentavam um ponto centralizado de falha; ou 2) não superavam o chamado problema do “gasto duplo”. O Bitcoin, por outro lado, era absolutamente não reproduzível e construído de tal modo que seu registro histórico de transações possibilitava que cada unidade monetária fosse conciliada e verificada no decorrer da evolução da moeda. Ademais, e o que era essencial, a moeda residia em uma rede de código-fonte aberto, não sendo propriedade de ninguém em particular, removendo, assim, o problema de um ponto único de falha. Havia outros elementos também: a criptografia, uma rede distribuída, e um desenvolvimento contínuo tornado possível por meio de desenvolvedores pagos pelos serviços de verificação de transações por eles providos.

Dificilmente passa um dia sem que eu – assim como muitos outros – me maravilhe na formidável genialidade desse sistema; tão meticuloso, tão aparentemente completo, tão puro. Muitas pessoas, até mesmo economistas da Escola Austríaca, estavam convencidas da impossibilidade de reinventar o dinheiro em bases privadas (F. A. Hayek foi a grande exceção, tendo sugerido a ideia ao redor de 1974). Entretanto, tornou-se um fato inegável que o Bitcoin existia e obtinha um valor de mercado. Dois anos após ter sido lançado ao mundo, o bitcoin atingiu a paridade com o dólar americano – algo imaginado como possível por muito poucos.

Hoje reverenciamos o acontecimento. Temos diante de nós mesmos uma moeda internacional emergente, criada inteiramente pelas forças de mercado. O sistema está sendo reformado não porque banqueiros centrais o desejem, não por causa de uma conferência internacional, tampouco porque um grupo de acadêmicos se reuniu e formulou um plano. Está sendo reformado, na verdade, de fora para dentro e de baixo para cima, baseado nos princípios do empreendedorismo e das trocas de mercado. É realmente incrível o quanto todo o processo que se desenrola diante de nosso testemunho se conforma ao modelo delineado pela teoria da origem do dinheiro de Carl Menger. Há apenas uma diferença, que surpreendeu o mundo: a base do valor do Bitcoin jaz não no seu uso prévio no escambo, conforme Menger descreveu, mas sim no seu uso atual como um sistema de pagamento. Quão privilegiados somos de testemunhar esse acontecimento no nosso tempo!

E qual é o potencial? O Bitcoin tem todas as melhores características do melhor dinheiro, sendo escasso, divisível, portátil, mas vai, inclusive, além na direção do ideal monetário, por ser ao mesmo tempo “sem peso e sem espaço” – é incorpóreo. Isso possibilita a transferência de propriedade a despeito da geografia a um custo virtualmente nulo e sem depender de um terceiro intermediário, contornando, dessa forma, todo o sistema bancário completamente subvertido pela intervenção governamental. O Bitcoin, então, propicia a perspectiva de restaurar a solidez e o universalismo do padrão-ouro do mundo antigo, além de aprimorá-lo por existir fora do controle direto do governo. Isso é, mais uma vez, digno de admiração.

Muitos têm alertado que governos não tolerarão que o sistema monetário seja reformado por um punhado de cyberpunks e seu dinheiro mágico de internet. Haverá intervenções. Haverá regulações. Haverá taxações. Haverá também tentativas de controlar. Mas olhemos a história recente. Governos tentaram impedir e então nacionalizar os correios. Buscaram impedir o compartilhamento de arquivos. Procuraram acabar com a pirataria. Tentaram também suspender a distribuição online de fármacos. Tentaram acabar com o uso, a fabricação e distribuição online

de drogas. Buscaram gerir e controlar o desenvolvimento de software por meio de patentes e leis antitruste. Se tentarem barrar ou até mesmo controlar uma criptomoeda, não terão êxito. Serão novamente derrotados pelas forças de mercado.

E aqui está a ironia. A forma mais direta com a qual os governos podem controlar o Bitcoin é intervindo na conversão entre a moeda digital e as moedas nacionalizadas. Quanto mais eles intervêm, mais eles incentivam os indivíduos a mover-se ao e permanecer no ecossistema do Bitcoin. Todas essas tentativas poderiam acabar alimentando o mercado. Mas há outras razões, além dessa consideração, que fazem de uma criptomoeda algo irreversível: taxas de transações praticamente nulas, segurança, proteção contra fraude, velocidade, privacidade e muito mais. Bitcoin é simplesmente uma tecnologia superior.

Cem anos atrás, o desenvolvimento da moeda foi retirado das forças de mercado e posto nas mãos dos governos. As consequências foram guerra, instabilidade econômica, o furto dos poupadores, exploração em massa e a explosão do poder e tamanho dos estados ao redor de todo o mundo. A criptomoeda proporciona a perspectiva de não somente reverter essas tendências, mas, também, de jogar um papel crucial na construção de um novo mundo de liberdade.

O que podemos todos nós aprender com a recente história do Bitcoin? Seja honesto: praticamente ninguém pensou que isso seria possível. Os mercados provaram o contrário. A lição nos ensina a sermos humildes, a olharmos para fora da janela, estando dispostos a sermos surpreendidos, deferindo aos resultados da ação humana, e nunca deixarmos nossa teoria interferir no nosso entendimento, e esperarmos que o mercado entregue muito mais do que jamais imaginamos ser possível.

Por tudo isso é tão importante o livro que você tem em mãos. Publicado pelo prestigioso Instituto Ludwig von Mises Brasil, nesta obra Fernando Ulrich explica o funcionamento e o potencial do Bitcoin em relação ao futuro da moeda, da política nacional e da própria liberdade humana.

Introdução

À PRIMEIRA VISTA, ENTENDER O QUE É BITCOIN não é uma tarefa fácil. A tecnologia é tão inovadora, abarca tantos conceitos de distintos campos do conhecimento humano – e, além disso, rompe inúmeros paradigmas – que explicar o fenômeno pode ser uma missão ingrata.

Em poucas palavras, o Bitcoin é uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações online, é a forma ideal de pagamento, pois é rápido, barato e seguro. Você lembra como a internet e o e-mail revolucionaram a comunicação? Antes, para enviar uma mensagem a uma pessoa do outro lado da Terra, era necessário fazer isso pelos correios. Nada mais antiquado. Você dependia de um intermediário para, fisicamente, entregar uma mensagem. Pois é, retornar a essa realidade é inimaginável. O que o e-mail fez com a informação, o Bitcoin fará com o dinheiro. Com o Bitcoin você pode transferir fundos de A para B em qualquer parte do mundo sem jamais precisar confiar em um terceiro para essa simples tarefa. É uma tecnologia realmente inovadora.

Mas como ele funciona na prática? Quais os benefícios e desafios do Bitcoin? A primeira parte desta obra é dedicada justamente a explicar o que é a tecnologia, suas principais características e como ela opera, bem como as suas vantagens e desafios. Será possível entender os detalhes de seu funcionamento e algumas das implicações dessa inovação tecnológica.

Entendido o básico sobre o Bitcoin, partiremos ao capítulo seguinte, buscando compreender o contexto e a história do surgimento da tecnologia. Muito mais do que algo aparentemente repentino, veremos como o Bitcoin é fruto de anos de intensa pesquisa em ciência da computação. Procuraremos contextualizar o aparecimento do Bitcoin, abordando em detalhes a ordem monetária atual e sua evolução até o presente. Será possível entender não apenas o altíssimo nível de intervenção presente no sistema financeiro moderno, mas também como o Bitcoin é uma resposta direta a esse estado de coisas.

Concluído esse capítulo, entraremos na parte mais densa desta obra, dedicada especialmente aos economistas, em que aplicaremos todo o ferramental teórico da ciência econômica – alicerçado principalmente na teoria monetária desenvolvida por Ludwig von Mises – para analisar o fenômeno Bitcoin sob todos os ângulos possíveis[1]. Como veremos adiante, a compreensão do seu surgimento no mercado e das suas particularidades e vantagens comparadas às formas de moeda hoje existentes nos permitirá realizar uma análise do Bitcoin plena e fundamentada. Abordando peculiaridades desde a falta de lastro, até a intangibilidade, a oferta inelástica e a ausência de um emissor central, etc., será possível aperfeiçoar o entendimento não somente do Bitcoin, mas, até mesmo, da própria noção de dinheiro no sentido estritamente econômico do termo. Encerraremos esse capítulo revisitando a definição de moeda como é comumente entendida, propondo, inclusive, um refinamento dela.

Por fim, defenderemos, na última parte do livro, o ideal de liberdade monetária, demonstrando a sua imprescindibilidade a qualquer sociedade que almeje a prosperidade e a paz – ideal pelo qual renomados economistas liberais lutaram durante décadas, tendo todos, igualmente, fracassado. Aproveitaremos esse momento para expor nossas conclusões sobre o porquê desses sucessivos malogros e, finalmente, compreender a essência do Bitcoin e como ele se encaixa nesse cenário. O futuro da moeda será o pano de fundo para a conclusão da obra.

Embora este livro seja uma introdução do Bitcoin ao público leigo, ele é, sobretudo, uma obra de ciência econômica aplicada à mais recente inovação no âmbito monetário. Espero, portanto, que ele possa contribuir ao progresso da economia, agregando perspectivas originais e aprimorando o entendimento dos fenômenos monetários segundo a tradição da Escola Austríaca iniciada por Carl Menger.

Em definitivo, o Bitcoin é a maior inovação tecnológica desde a internet, é revolucionário, sem precedentes e tem o potencial de mudar o mundo de uma forma jamais vista. À moeda, ele é o futuro. Ao avanço da liberdade individual, é uma esperança e uma grata novidade.

Boa leitura,
10 de fevereiro de 2014.
Fernando Ulrich

Rodapé

---

1 Àqueles que detêm pouco conhecimento em economia, poderá ser um pouco difícil acompanhar esse capítulo, embora tenhamos nos esforçado para deixá-lo o mais palatável possível.

Bitcoin: o que é e como funciona

1. O que é Bitcoin

BITCOIN É UMA MOEDA DIGITAL *peer-to-peer* (par a par ou, simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central. Entre muitas outras coisas, o que faz o Bitcoin ser único é o fato de ele ser o primeiro sistema de pagamentos global totalmente descentralizado. Ainda que à primeira vista possa parecer complicado, os conceitos fundamentais não são difíceis de compreender.[2]

Visão geral

Até a invenção do Bitcoin, em 2008, pelo programador não identificado conhecido apenas pelo nome Satoshi Nakamoto, transações online sempre requereram um terceiro intermediário de confiança. Por exemplo, se Maria quisesse enviar 100 u.m. ao João por meio da internet, ela teria que depender de serviços de terceiros como PayPal ou Mastercard. Intermediários como o PayPal mantêm um registro dos saldos em conta dos clientes. Quando Maria envia 100 u.m ao João, o PayPal debita a quantia de sua conta, creditando-a na de João. Sem tais intermediários, um dinheiro digital poderia ser gasto duas vezes. Imagine que não haja intermediários com registros históricos, e que o dinheiro digital seja simplesmente um arquivo de computador, da mesma forma que documentos digitais são arquivos de computador. Maria poderia enviar ao João 100 u.m. simplesmente anexando o arquivo de dinheiro em uma mensagem. Mas assim como ocorre com um e-mail, enviar um arquivo como anexo não o remove do computador originador da mensagem eletrônica. Maria reteria a cópia do arquivo após tê-lo enviado anexado à mensagem. Dessa forma, ela poderia facilmente enviar as mesmas 100 u.m. ao Marcos. Em ciência da computação, isso é conhecido como o problema do "gasto duplo", e, até o advento do Bitcoin, essa questão só poderia ser solucionada por meio de um terceiro de confiança que empregasse um registro histórico de transações.

A invenção do Bitcoin é revolucionária porque, pela primeira vez, o problema do gasto duplo pode ser resolvido sem a necessidade de um terceiro; Bitcoin o faz distribuindo o imprescindível registro histórico a todos os usuários do sistema via uma rede *peer-to-peer.* Todas as transações que ocorrem na economia Bitcoin são registradas em uma espécie de livro-razão[3] público e distribuído chamado de *blockchain* (corrente de blocos, ou simplesmente um registro público de transações), o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações realizadas. Novas transações são verificadas contra o *blockchain* de modo a assegurar que os mesmos bitcoins[4] não tenham sido previamente gastos, eliminando assim o problema do gasto duplo. A rede global *peer-to-peer*, composta de milhares de usuários, torna-se o próprio intermediário; Maria e João podem transacionar sem o PayPal.

É importante notar que as transações na rede Bitcoin não são denominadas em dólares, euros ou reais, como são no PayPal ou Mastercard; em vez disso, são denominadas em bitcoins. Isso torna o sistema Bitcoin não apenas uma rede de pagamentos decentralizada, mas também uma moeda virtual. O valor da moeda não deriva do ouro ou de algum decreto governamental, mas do valor que as pessoas lhe atribuem. O valor em reais de um bitcoin é determinado em um mercado aberto, da mesma forma que são estabelecidas as taxas de câmbio entre diferentes

moedas mundiais.

Como funciona

Até aqui discutimos o que é o Bitcoin: uma rede de pagamentos *peer-to-peer* e uma moeda virtual que opera, essencialmente, como o dinheiro online. Vejamos agora como é seu funcionamento.

As transações são verificadas, e o gasto duplo é prevenido, por meio de um uso inteligente da criptografia de chave pública. Tal mecanismo exige que a cada usuário sejam atribuídas duas "chaves", uma privada, que é mantida em segredo, como uma senha, e outra pública, que pode ser compartilhada com todos. Quando a Maria decide transferir bitcoins ao João, ela cria uma mensagem, chamada de "transação", que contém a chave pública do João, assinando com sua chave privada. Olhando a chave pública da Maria, qualquer um pode verificar que a transação foi de fato assinada com sua chave privada, sendo, assim, uma troca autêntica, e que João é o novo proprietário dos fundos. A transação – e portanto uma transferência de propriedade dos bitcoins – é registrada, carimbada com data e hora e exposta em um "bloco" do *blockchain* (o grande banco de dados, ou livro-razão da rede Bitcoin). A criptografia de chave pública garante que todos os computadores na rede tenham um registro constantemente atualizado e *verificado* de todas as transações dentro da rede Bitcoin, o que impede o gasto duplo e qualquer tipo de fraude.

Mas o que significa dizermos que "a rede" verifica as transações e as reconcilia com o registro público? E como exatamente são criados e introduzidos novos bitcoins na oferta monetária? Como vimos, porque o Bitcoin é uma rede *peer-to-peer*, não há uma autoridade central encarregada nem de criar unidades monetárias nem de verificar as transações. Essa rede depende dos usuários que proveem a força computacional para realizar os registros e as reconciliações das transações. Esses usuários são chamados de "mineradores"[5], porque são recompensados pelo seu trabalho com bitcoins recém-criados. Bitcoins são criados, ou "minerados", à medida que milhares de computadores dispersos resolvem problemas matemáticos complexos que verificam as transações no *blockchain*. Como um analista afirmou,

> A real mineração de bitcoins é puramente um processo matemático. Uma analogia útil é a procura de números primos: costumava ser relativamente fácil achar os menores (Erastóstenes, na Grécia Antiga, produziu o primeiro algoritmo para encontrá-los). Mas à medida que eles eram encontrados, ficava mais difícil encontrar os maiores. Hoje em dia, pesquisadores usam computadores avançados de alto desempenho para encontrá-los, e suas façanhas são observadas pela comunidade da matemática (por exemplo, a Universidade do Tennessee mantém uma lista dos 5.000 maiores).
>
> No caso do Bitcoin, a busca não é, na verdade, por números primos, mas por encontrar a sequência de dados (chamada de "bloco") que produz certo padrão quando o algoritmo "*hash*" do Bitcoin é aplicado aos dados. Quando uma combinação ocorre, o minerador obtém um prêmio de bitcoins (e também uma taxa de serviço, em bitcoins, no caso de o mesmo bloco ter sido usado para verificar uma transação). O tamanho do prêmio é reduzido ao passo que bitcoins são minerados.
>
> A dificuldade da busca também aumenta, fazendo com que seja computacionalmente mais difícil encontrar uma combinação. Esses dois efeitos combinados acabam por reduzir ao longo do tempo a taxa com que bitcoins são produzidos, imitando a taxa de produção de uma commodity como o ouro. Em um momento futuro, novos bitcoins não serão produzidos, e o único incentivo aos mineradores serão as taxas de serviços pela

verificação de transações[6].

O protocolo, portanto, foi projetado de tal forma que cada minerador contribui com a força de processamento de seu computador visando à sustentação da infraestrutura necessária para manter e autenticar a rede da moeda digital. Mineradores são premiados com bitcoins recém-criados por contribuir com força de processamento para manter a rede e por verificar as transações no *blockchain*. E à medida que mais capacidade computacional é dedicada à mineração, o protocolo incrementa a dificuldade do problema matemático, assegurando que bitcoins sejam sempre minerados a uma taxa previsível e limitada.

Esse processo de mineração de bitcoins não continuará indefinidamente. O Bitcoin foi projetado de modo a reproduzir a extração de ouro ou outro metal precioso da Terra – somente um número limitado e previamente conhecido de bitcoins poderá ser minerado. A quantidade arbitrária escolhida como limite foi de 21 milhões de bitcoins. Estima-se que os mineradores colherão o último “satoshi”, ou 0,00000001 de um bitcoin, no ano de 2140. Se a potência de mineração total escalar a um nível bastante elevado, a dificuldade de minerar bitcoins aumentará tanto que encontrar o último “satoshi” será uma empreitada digital consideravelmente desafiadora. Uma vez que o último “satoshi” tenha sido minerado, os mineradores que direcionarem sua potência de processamento ao ato de verificação das transações serão recompensados com taxas de serviço, em vez de novos bitcoins minerados. Isso garante que os mineradores ainda tenham um incentivo de manter a rede operando após a extração do último bitcoin.

O uso de pseudônimo

Muita atenção midiática é dada ao suposto anonimato que a moeda digital permite aos seus usuários. Essa ideia, no entanto, deriva de um errôneo entendimento do Bitcoin. Porque as transações online até hoje necessitaram de um terceiro intermediário, elas não foram anônimas. O PayPal, por exemplo, tem um registro de todas as vezes em que a Maria enviou dinheiro ao João. E porque as contas no PayPal da Maria e do João são amarradas a suas contas bancárias, suas identidades são provavelmente sabidas. Em contraste, se a Maria entrega ao João 100 reais em dinheiro, não há intermediário nem registro da transação. E se a Maria e o João não conhecem um ao outro, podemos dizer que a transação é completamente anônima.

O Bitcoin encaixa-se em algum ponto entre esses dois extremos. Por um lado, bitcoins são como dinheiro vivo, no sentido de que, quando a Maria envia bitcoins ao João, ela não mais os possui, e ele sim, e não há nenhum terceiro intermediário entre eles que conhece suas respectivas identidades. Por outro lado, e diferentemente do dinheiro vivo, o fato de que a transação ocorreu entre duas chaves públicas, em tal dia e hora, com certa quantidade, além de outras informações, é registrado no *blockchain*. Em realidade, qualquer e toda transação já efetuada na história da economia Bitcoin pode ser vista no *blockchain*.

Enquanto as chaves públicas de todas as transações – também conhecidas como “endereços Bitcoin”[7] – são registradas no *blockchain*, tais chaves não são vinculadas à identidade de ninguém. Porém, se a identidade de uma pessoa estivesse associada a uma chave pública, poderíamos vasculhar as transações no *blockchain* e facilmente ver todas as transações associadas a essa chave. Dessa forma, ainda que Bitcoin seja bastante semelhante ao dinheiro vivo, em que as partes podem transacionar sem revelar suas identidades a um terceiro ou entre si, é também distinto do dinheiro vivo, pois todas as transações de e para um endereço Bitcoin qualquer podem ser rastreadas. Nesse sentido, Bitcoin não garante o anonimato, mas permite o uso de pseudônimo.

Vincular uma identidade do mundo real a um endereço Bitcoin não é tão difícil quanto se possa imaginar. Para começar, a identidade de uma pessoa (ou pelo menos informação de identificação, como um endereço IP) é frequentemente registrada quando alguém realiza uma transação de Bitcoin em uma página web ou troca dólares por bitcoins em uma casa de câmbio de bitcoins. Para aumentar as chances de manter o pseudônimo, seria necessário empregar softwares de anonimato como Tor, e ter o cuidado de nunca transacionar com um endereço Bitcoin no qual poderia ser rastreada a identidade do usuário.

Por fim, é também possível colher identidades simplesmente olhando o *blockchain*. Um estudo descobriu que técnicas de agrupamento baseadas em comportamento poderiam revelar as identidades de 40% dos usuários de Bitcoin em um experimento simulado. Uma pesquisa mais antiga das propriedades estatísticas do gráfico de transações de Bitcoin mostrou como uma análise passiva da rede com as ferramentas apropriadas pode revelar a atividade financeira e as identidades de usuários de Bitcoin.

Já uma análise recente das propriedades estatísticas do gráfico de transações de bitcoins colheu resultados similares ao de um banco de dados mais abrangente. Uma outra análise do gráfico de transações de bitcoins reiterou que observadores usando "fusão de entidade"[8] podem notar padrões estruturais no comportamento do usuário, enfatizando que esse "é um dos desafios mais importantes ao anonimato do Bitcoin".[9] Apesar disso, usuários de Bitcoin desfrutam de um nível muito maior de privacidade do que usuários de serviços tradicionais de transferência digital, os quais precisam fornecer informação pessoal detalhada a terceiros intermediários que facilitam a troca financeira.

Ainda que Bitcoin seja frequentemente referido como uma moeda "anônima", em realidade, é bastante difícil permanecer anônimo na rede Bitcoin. Pseudônimos ligados a transações protocoladas no registro público podem ser identificados anos após a realização de uma troca. Uma vez que intermediários de Bitcoin[10] estejam completamente em dia com as regulações requeridas a intermediários financeiros tradicionais, o anonimato será ainda menos garantido, porque dos intermediários de Bitcoin será exigido coletar dados pessoais de seus clientes.

2. Benefícios do Bitcoin

A primeira pergunta que muitas pessoas fazem quando aprendem sobre Bitcoin é: por que eu usaria bitcoins quando posso usar reais (ou dólares)? Bitcoin ainda é uma moeda nova e flutuante que não é aceita por muitos comerciantes, tornando seus usos quase experimentais. Para entender melhor o Bitcoin, ajuda se pensarmos que ele não é necessariamente um substituto às moedas tradicionais, mas sim um novo sistema de pagamentos.

Menores custos de transação

Porque não há um terceiro intermediário, as transações de Bitcoin são substancialmente mais baratas e rápidas do que as feitas por redes de pagamentos tradicionais. E porque as transações são mais baratas, o Bitcoin faz com que micropagamentos e suas inovações sejam possíveis. Adicionalmente, o Bitcoin é uma grande promessa de uma forma de reduzir os custos de transação aos pequenos comerciantes e remessas de dinheiro globais, aliviar a pobreza global pelo facilitado acesso ao capital, proteger indivíduos contra controles de capitais e censura, garantir privacidade financeira a grupos oprimidos e estimular a inovação (dentro e acima do protocolo Bitcoin). Por outro lado, a natureza descentralizada do Bitcoin também apresenta

oportunidades ao crime. O desafio, então, é desenvolver processos que reduzam as oportunidades para criminalidade enquanto mantêm-se os benefícios que Bitcoin oferece.

Em primeiro lugar, Bitcoin é atrativo a pequenas empresas de margens apertadas que procuram formas de reduzir seus custos de transação na condução de seus negócios. Cartões de crédito expandiram de forma considerável a facilidade de transacionar, mas seu uso vem acompanhado de pesados custos aos comerciantes. Negócios que desejam oferecer aos seus clientes a opção de pagamento com cartões de crédito precisam, primeiro, contratar uma conta com as empresas de cartões. Dependendo dos termos de acordo com cada empresa, os comerciantes têm de pagar uma variedade de taxas de autorização, taxas de transação, taxas de extrato, etc. Essas taxas rapidamente se acumulam e aumentam significativamente o custo dos negócios. Entretanto, se um comerciante rejeita aceitar pagamentos com cartões de crédito, pode perder um número considerável de suas vendas a clientes que preferem o uso de tal comodidade.

Como Bitcoin facilita transações diretas sem um terceiro, ele remove cobranças custosas que acompanham as transações com cartões de crédito. O Founders Fund, um fundo de *venture capital* encabeçado por Peter Thiel, do PayPal e Facebook, recentemente investiu 3 milhões de dólares na companhia de processamento de pagamentos BitPay, por causa da habilidade do serviço em reduzir os custos no comércio online internacional. De fato, pequenos negócios já começaram a aceitar bitcoins como uma forma de evitar os custos de operar com empresas de cartões de crédito. Outros adotaram a moeda pela sua velocidade e eficiência em facilitar as transações. O Bitcoin provavelmente continuará a reduzir os custos de transações das empresas que o aceitam à medida que mais e mais pessoas o adotem.

Aceitar pagamentos com cartões de crédito também sujeita as empresas ao risco de fraude de estorno de pagamentos (*charge-back fraud*). Há muito que comerciantes têm sido infestados por estornos fraudulentos, ou reversões de pagamentos iniciadas por clientes, baseados no falso pretexto de que o produto não foi entregue[11]. Comerciantes, portanto, podem perder o pagamento pelo item vendido, além do próprio item, e ainda terão de pagar uma taxa pelo estorno. Como um sistema de pagamentos não reversível, o Bitcoin elimina a “fraude amigável” acarretada pelo mau uso de estornos de consumidores. Aos pequenos negócios, isso pode ser fundamental.

Consumidores gostam dos estornos, no entanto, porque o sistema os protege de erros de comerciantes, inescrupulosos ou não. Consumidores podem também gozar dos outros benefícios que os cartões de crédito oferecem. E muitos consumidores e comerciantes provavelmente preferiram ater-se aos serviços tradicionais de cartões de crédito, mesmo com a disponibilidade dos pagamentos pela rede Bitcoin. Ainda assim, a ampliação do leque de escolhas de opções de pagamento beneficiaria a todos os gostos.

Aqueles que querem a proteção e as regalias do uso do cartão de crédito podem continuar a operar assim, mesmo que isso signifique pagar um pouco mais. Aqueles mais sensíveis ao preço ou à privacidade podem usar bitcoins. Não ter de pagar taxas às companhias de cartões de crédito significa que os comerciantes podem repassar as economias aos preços finais ao consumidor. Exatamente nesse modelo de negócios trabalha a loja Bitcoin Store, que vende milhares de eletrônicos com grandes descontos, aceitando como pagamento somente bitcoins[12].

Como um acessível sistema de transferência de fundos, Bitcoin também é uma grande promessa ao futuro das remessas de dinheiro de baixo custo. Em 2012, imigrantes de países desenvolvidos enviaram pelo menos 401 bilhões de dólares em remessas ao seus parentes vivendo em países em desenvolvimento[13]. Estima-se que a quantidade de remessas aumente

para 515 bilhões de dólares por volta de 2015[14]. A maior parte dessas remessas é enviada usando serviços tradicionais como Western Union ou a MoneyGram, que cobram pesadas taxas, além de demorar diversos dias úteis para concluir a transferência dos fundos. No primeiro trimestre de 2013, a taxa média pelo serviço girou em torno de 9%[15]. Em contraste, as taxas de transações na rede Bitcoin tendem a ser menos de 0,0005 BTC[16], ou 1% da transação. Essa oportunidade empreendedora de melhorar as transferências de dinheiro tem atraído grandes nomes do universo de investidores de *venture capital*. Até mesmo a MoneyGram e a Western Union estão analisando se integram o Bitcoin ao seu modelo de negócios. O Bitcoin permite remessas baratas e instantâneas, e a redução de custo dessas remessas aos consumidores pode ser considerável.

Potencial arma contra a pobreza e a opressão

Bitcoin também tem o potencial de melhorar a qualidade de vida dos mais pobres no mundo. Aumentar o acesso a serviços financeiros básicos é uma técnica antipobreza promissora[17]. De acordo com estimativas, 64% das pessoas vivendo em países em desenvolvimento têm parco acesso a esses serviços, talvez porque seja bastante custoso a instituições financeiras tradicionais servir às áreas pobres e rurais[18].

Por causa dos empecilhos ao desenvolvimento de serviços bancários tradicionais em áreas pobres, pessoas em países em desenvolvimento têm recorrido aos serviços bancários via rede de telefonia móvel para fazer frente às necessidades financeiras. O sistema fechado de pagamentos por celular M-Pesa tem sido particularmente exitoso em países como Quênia, Tanzânia e Afeganistão[19]. Empreendedores já estão se movendo rumo a esse modelo; o serviço de carteira de Bitcoin Kipochi recentemente desenvolveu um produto que permite a usuários do M-Pesa trocar bitcoins[20]. Serviços bancários por celular em países em desenvolvimento podem ser ampliados pela adoção do Bitcoin. Como um sistema aberto de pagamentos, o Bitcoin pode fornecer às pessoas nesses locais acesso barato a serviços financeiros, em uma escala global.

O Bitcoin pode também propiciar alívio às pessoas vivendo em nações com controles de capitais bastante estritos. O número total de bitcoins que podem ser minerados é limitado e não pode ser manipulado. Não há autoridade central que possa reverter transações e impedir a troca de bitcoins entre países. O Bitcoin, dessa forma, proporciona uma válvula de escape para pessoas que almejam uma alternativa à moeda depreciada de seu país ou a mercados de capitais estrangulados. Já há casos de pessoas recorrendo ao Bitcoin para evadir-se dos efeitos danosos dos controles de capitais e da má gestão de bancos centrais. Alguns argentinos, por exemplo, adotaram o Bitcoin em resposta ao duplo fardo do país, taxas de inflação de mais de 25% ao ano e rigorosos controles de capitais[21]. A demanda por bitcoins é tão grande na Argentina que uma popular casa de câmbio está planejando abrir um escritório no país[22]. O uso de bitcoins naquele país continua crescendo em face da péssima ingerência estatal no âmbito monetário.

Indivíduos em situações de opressão ou emergência também podem beneficiar-se da privacidade financeira que o Bitcoin proporciona. Há muitas razões legítimas pelas quais pessoas buscam privacidade em suas transações financeiras. Esposas fugindo de parceiros abusivos precisam de alguma forma de discretamente gastar seu dinheiro sem ser rastreadas. Pessoas procurando serviços de saúde controversos desejam privacidade de familiares, empregadores e outros que podem julgar suas decisões. Experiências recentes com governos despóticos sugerem que cidadãos oprimidos se beneficiaram altamente da possibilidade de realizar transações privadas, livres das garras de tiranos. O Bitcoin oferece algo de privacidade

como a que tem sido tradicionalmente permitida pelo uso de dinheiro vivo – com a conveniência adicional de transferência digital.

Estímulo à inovação financeira

Uma das aplicações mais promissoras do Bitcoin é como uma plataforma à inovação financeira. O protocolo do Bitcoin contém o modelo de referência digital para uma quantidade de serviços financeiros e legais úteis que programadores podem desenvolver facilmente. Como bitcoins são, no seu cerne, simplesmente pacotes de dados, eles podem ser usados para transferir não somente moedas, mas também ações de empresas, apostas e informações delicadas[23]. Alguns dos atributos que estão embutidos no protocolo do Bitcoin incluem micropagamentos, mediações de litígios, contratos de garantia e propriedade inteligente[24]. Esses atributos permitiriam o fácil desenvolvimento de serviços de tradução via internet, processamento instantâneo de transações pequenas (como medição automática de acesso Wi-Fi) e serviços de *crowdfunding*[25].

Adicionalmente, programadores podem desenvolver protocolos alternativos em cima do protocolo do Bitcoin da mesma forma que a *web* e o correio eletrônico operam no protocolo da internet TCP/IP. Um programador já propôs uma nova camada de protocolo para agregar ao protocolo do Bitcoin e assim aperfeiçoar a estabilidade e segurança da rede[26]. Outro criou um serviço de tabelião digital para armazenar anonimamente e com segurança uma "prova de existência" para documentos privados, em cima do protocolo do Bitcoin[27]. Outros, ainda, adotaram o modelo Bitcoin como forma de cifrar comunicações de correio eletrônico[28]. Um grupo de desenvolvedores esboçou um protocolo aditivo que melhorará a privacidade da rede[29]. O Bitcoin é, portanto, a fundação sobre a qual outras camadas de funcionalidade podem ser construídas. O projeto Bitcoin pode ser mais bem imaginado como um processo de experimentação financeira e comunicativa. Os elaboradores de políticas públicas devem ter cuidado para que suas diretivas não suprimam as inovações promissoras em desenvolvimento dentro e sobre o novato protocolo.

3. Desafios do Bitcoin

Apesar dos benefícios que ele apresenta, o Bitcoin tem algumas desvantagens que usuários em potencial devem levar em consideração. Houve significativa volatilidade no preço ao longo de sua existência. Novos usuários correm o risco de não proteger devidamente suas carteiras ou de, até mesmo, acidentalmente apagar seus bitcoins, caso não sejam cautelosos. Além disso, há preocupações sobre se *hackers* podem de alguma forma comprometer a economia Bitcoin.

Volatilidade

O Bitcoin foi exposto a pelo menos cinco ajustes de preço significativos desde 2011[30]. Esses ajustes se assemelham a bolhas especulativas tradicionais: coberturas da imprensa otimistas em demasia provocam ondas de investidores novatos a pressionar para cima o preço do bitcoin[31]. A exuberância, então, atinge um ponto de inflexão, e o preço finalmente despenca. Novos entrantes ávidos por participar correm o risco de sobrevalorizar a moeda e perder dinheiro em uma queda abrupta. O valor flutuante do bitcoin faz com que muitos observadores permaneçam céticos quanto ao futuro da moeda.

Será que essa volatilidade prediz o fim do Bitcoin? Alguns analistas acham que sim[32]. Outros sugerem que essas flutuações acabam por realizar testes de estresse à moeda e podem, por fim, diminuir em frequência à medida que mecanismos para contrabalancear a volatilidade se desenvolvem[33]. Se bitcoins são usados apenas como reserva de valor ou unidade de conta, a volatilidade poderia de fato ameaçar seu futuro. Não faz sentido gerir as finanças de um negócio ou guardar as economias em bitcoins se o preço de mercado oscila desenfreada e imprevisivelmente. Quando o Bitcoin é empregado como meio de troca, entretanto, a volatilidade não é tanto um problema. Comerciantes podem precificar seus produtos em termos de moeda tradicional e aceitar o equivalente em bitcoins. Clientes que adquirem bitcoins para realizar uma só compra não se importam com o câmbio amanhã; eles somente se preocupam com que o Bitcoin reduza custos de transações no presente. A utilidade do Bitcoin como meio de troca poderia explicar por que a moeda tem se tornado popular entre comerciantes, a despeito da volatilidade de seu preço[34]. É possível que o valor de bitcoins venha a apresentar uma menor volatilidade ao passo que mais pessoas se familiarizam com sua tecnologia e desenvolvam expectativas realistas acerca de seu futuro.

Violação de segurança

Como uma moeda digital, o Bitcoin apresenta alguns desafios de segurança específicos[35]. Se as pessoas não são cuidadosas, elas podem inadvertidamente apagar ou perder seus bitcoins. Uma vez que o arquivo digital esteja perdido, o dinheiro está perdido, da mesma forma com dinheiro vivo de papel. Se as pessoas não protegem seus endereços Bitcoin, elas podem estar mais sujeitas ao roubo. As carteiras de Bitcoin agora podem ser protegidas por criptografia, mas os usuários devem selecionar a ativação da criptografia. Se um usuário não cifra a sua carteira, os bitcoins podem ser roubados por *malware*[36]. As casas de câmbio de Bitcoin também enfrentaram complicações de segurança; *hackers* furtaram 24 mil BTC (então valorados em 250 mil dólares) de um casa de câmbio chamada Bitfloor em 2012[37], e houve em uma série de ataques DDoS (*distributed denial-of-service*) contra a mais popular casa de câmbio, Mt.Gox, em 2013[38]. (A Bitfloor finalmente repagou os fundos roubados aos clientes, e a Mt.Gox recuperou-se de tais ataques). Obviamente, muitos dos riscos de segurança enfrentados pelo Bitcoin são similares àqueles com os quais moedas tradicionais também se defrontam. Notas de reais podem ser destruídas ou perdidas, informação financeira pessoal pode ser roubada e usada por criminosos e bancos podem ser assaltados ou alvos de ataques DDoS. Os usuários de Bitcoin deveriam aprender sobre e como preparar-se contra riscos de segurança, da mesma forma que o fazem com outras atividades financeiras.

Uso para fins criminosos

Também há razões para os políticos ficarem apreensivos quanto a algumas das aplicações não intencionadas do Bitcoin. Porque o Bitcoin permite o uso de pseudônimos, políticos e jornalistas têm questionado se criminosos podem usá-lo para lavagem de dinheiro ou para aceitar pagamentos da venda de produtos e serviços ilícitos. De fato, e como o dinheiro vivo, ele pode ser usado tanto para o bem quanto para o mal. Um exemplo notório é o caso do site de mercado negro em *deep web*[39] conhecido como Silk Road[40]. Esse site se aproveitava da rede para anonimato Tor e da natureza de se usar pseudônimo no Bitcoin para disponibilizar um vasto mercado digital em que se podia encomendar drogas por correio, além de outros produtos lícitos e ilícitos. Ainda que os administradores do Silk Road não permitissem a troca de nenhum produto que resultasse de fraude ou dano, como cartões de crédito roubados ou fotos de exploração de menores, era permitido aos comerciantes vender produtos ilegais, como

documentos de identidade falsos e drogas ilícitas. O fato de se usar pseudônimo no Bitcoin permitia que compradores adquirissem produtos ilegais online, da mesma forma que o dinheiro tem sido tradicionalmente usado para facilitar compras ilícitas pessoalmente. Um estudo estimou que o total de transações mensais no Silk Road alcance aproximadamente 1,2 milhão de dólares[41]. Mas o mercado de Bitcoin acumulou 770 milhões de dólares em transações durante junho de 2013; vendas no Silk Road, portanto, constituíam uma quase insignificante parcela do total da economia Bitcoin[42].

A associação do Silk Road com o Bitcoin manchou sua reputação. Na sequência da publicação de um artigo sobre o Silk Road em 2011, os senadores norte-americanos Charles Schumer e Joe Manchin enviaram uma carta ao promotor-geral Eric Holder e ao administrador do *Drug Enforcement Administration*, Michele Leonhart, pedindo por uma caçada ao Silk Road, ao software de anonimato Tor e ao Bitcoin[43].

Outra preocupação é que o Bitcoin seja usado para a lavagem de dinheiro para o financiamento do terrorismo e tráfico de produtos ilegais. Apesar de essas inquietações serem, neste momento, mais teóricas do que empíricas, o Bitcoin poderia de fato ser uma opção àqueles que desejam mover dinheiro sujo discretamente. Preocupações com o potencial de o Bitcoin ser usado para lavagem de dinheiro foram atiçadas após o Liberty Reserve, um serviço privado e centralizado de moeda digital com sede na Costa Rica, ter sido encerrado pelas autoridades sob alegações de lavagem de dinheiro[44].

Embora o Liberty Reserve e o Bitcoin pareçam similares porque ambos oferecem moedas digitais, há diferenças importante entre os dois. O Liberty Reserve era um serviço de divisas centralizado, criado e pertencente a uma empresa privada, supostamente com o expresso propósito de facilitar a lavagem de dinheiro; o Bitcoin, não. As transações dentro da economia do Liberty Reserve não eram transparentes. O Bitcoin, por outro lado, é uma moeda descentralizada aberta que fornece um registro público de todas as transações. Lavadores de dinheiro podem tentar proteger seus endereços de Bitcoin e suas identidades, mas seus registros de transações serão sempre públicos e acessíveis a qualquer momento pelas autoridades. Lavar dinheiro por meio do Bitcoin, então, pode ser visto como uma empreitada muito mais arriscada do que usar um sistema centralizado como o Liberty Reserve. Ademais, diversas casas de câmbio de bitcoins têm tomado as medidas necessárias para estar em dia com as regulações e exigências das autoridades no que tange ao combate à lavagem de dinheiro[45]. A combinação de um sistema de registro público (o livro-razão do Bitcoin, ou o *blockchain*) com a cooperação das casas de câmbio na coleta de informações dos usuários fará do Bitcoin uma via relativamente menos atrativa aos lavadores de dinheiro.

Também é importante notar que muitas das potenciais desvantagens do Bitcoin são as mesmas enfrentadas pelo tradicional dinheiro vivo; este tem sido historicamente o veículo escolhido por traficantes e lavadores de dinheiro, mas políticos jamais seriamente considerariam banir o dinheiro vivo. À medida que os reguladores comecem a contemplar o Bitcoin, eles deveriam ser cautelosos com os perigos da regulação excessiva. No pior cenário possível, os reguladores poderiam impedir que negócios legítimos se beneficiem da rede Bitcoin sem impor nenhum empecilho ao uso do Bitcoin por traficantes ou lavadores de dinheiro. Se as casas de câmbio são sobrecarregadas pela regulação e encerram suas atividades, por exemplo, traficantes e afins ainda assim poderiam colocar dinheiro na rede, pagando uma pessoa com dinheiro vivo para que esta lhes transfira seus bitcoins. Nesse cenário, transações benéficas são impossibilitadas por regulação excessiva, enquanto as atividades-alvo continuam a ocorrer.

4. Regulação e legislação

As leis e regulações atuais não preveem uma tecnologia como o Bitcoin, o que resulta em algumas zonas legais cinzentas. Isso ocorre porque o Bitcoin não se encaixa em definições regulamentares existentes de moeda ou outros instrumentos financeiros ou instituições, tornando complexo saber quais leis se aplicam a ele e de que forma.

O Bitcoin tem as propriedades de um sistema eletrônico de pagamentos, uma moeda e uma commodity, entre outras. Dessa forma, estará certamente sujeito ao escrutínio de diversos reguladores. Vários países estão atualmente debatendo o Bitcoin em nível governamental. Alguns já emitiram pareceres ou pronunciamentos oficiais, estabelecendo diretrizes, orientações, etc. Uns com uma postura neutra, outros de forma mais cautelosa.

Embora não seja o foco deste livro averiguar qual o tratamento legal adequado, é oportuno afirmar que as questões legais certamente afetarão a forma como o Bitcoin se desenvolve ao redor do mundo. Em países desenvolvidos, as incertezas sobre como o Bitcoin será regulado pouco a pouco se dissolvem.

Mas em pleno ano de 2014, ainda há questões a serem endereçadas pelas autoridades. No Brasil, nada em específico concernente ao Bitcoin foi emitido pelos órgãos reguladores[46]. Por ser um mercado em franco e rápido crescimento, é de se esperar novidades no âmbito legal proximamente.

Rodapé

2 [Nota do autor]: Este segundo capítulo é uma tradução da obra de Jerry Brito e Andrea Castillo, “Bitcoin: A Primer for Policymakers” (Arlington, VA: Mercatus Center at George Mason University, 2013). A seção final sobre regulação foi reduzida visando adequá-la ao público brasileiro.

3 Livro-razão é nome dado pelos profissionais de contabilidade ao agrupamento dos registros contábeis de uma empresa que usa o método das partidas dobradas. Nele é possível visualizar todas as transações ocorridas em dado período de operação de uma empresa.

4 Quando nos referirmos ao sistema, à rede ou o ao projeto Bitcoin, usamos sempre inicial maiúscula. No entanto, quando fizermos referência às unidades monetárias bitcoins, utilizamos a palavra em caixa baixa.

5 Mineradores tendem a ser entusiastas da computação comuns, mas à medida que a mineração se torne mais difícil e cara, a atividade será, provavelmente, profissionalizada. Para maiores informações, ver LIU, Alec. A Guide to Bitcoin Mining. Motherboard, 2013. Disponível em: <http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600>. Acesso em: 10 dez. 2013.

6 TINDELL, Ken. Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995. Business Insider, 5 abr. 2013. Disponível em: <http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4>. Acesso em: 10 dez. 2013.

7 Bitcoin wiki “Address”. Disponível em: <https://en.bitcoin.it/wiki /Address>. Acesso em: 30 mar. 2013.

8 Fusão de entidade é o processo de observar duas ou mais chaves públicas usadas como um input a uma transação ao mesmo tempo. Assim, mesmo que um usuário tenha diversas chaves públicas distintas, um observador pode gradualmente vinculá-las e remover o ostensivo anonimato esperado de múltiplas chaves públicas

9 OBER, KATZENBEISSER e HAMACHER. Structure and Anonymity of the Bitcoin Transaction Graph. Future Internet 5, no. 2, 2013. Disponível em: <http://www.mdpi.com/1999-5903/5/2/237>. Acesso em: 10 dez. 2013.

10 Como exemplos de intermediários de Bitcoin, temos as casas de câmbio que facilitam a compra e venda entre moeda fiduciária e bitcoins. No Brasil, tais casas já solicitam uma quantidade de informações pessoais que pode desagradar a muitos usuários.

11 MALTBY, Emily. Chargebacks Create Business Headaches. Wall Street Journal, 10 fev. 2011. Disponível em: <http://online.wsj.com/article/SB10001424052748704698004
576104554234202010.html>. Acesso em: 10 dez. 2013.

12 O mesmo Samsung Galaxy Note que vende-se por US$ 779 na Amazon mais postagem é vendido na Bitcoin Store por

meros US$ 480,25. Dessa forma, Bitcoin oferece mais opções de baixo custo a consumidores e pequenas empresas sem remover a opção de uso de cartão de crédito daqueles que o preferem. BUTERIN, Vitalik. Bitcoin Store Opens: All Your Electronics Cheaper with Bitcoins. Bitcoin Magazine, 5 nov. 2012. Disponível em: <http://bitcoinmagazine.com/bitcoin-store-opens-all-your-electronics-cheaper-with-bitcoins/>. Acesso em: 10 dez. 2013.

13 World Bank Payment Systems Development Group, Remittance Prices Worldwide: An Analysis of Trends in the Average Total Cost of Migrant Remittance Services, Washington, DC, World Bank, 2013. Disponível em: <http://remittanceprices.worldbank.org/~/media/FPDKM/Remittances/Documents/RemittancePriceWorldwide-Analysis-Mar2013.pdf>. Acesso em: 11 dez. 2013.

14 Ibid.

15 Ibid.

16 Bitcoin wiki "Transaction fees". Disponível em: <https://en.bitcoin.it/wiki/Transaction_fees>. Acesso em: 11 dez. 2013. PAUL, Andrew. Is Bitcoin the Next Generation of Online Payments? Yahoo! Small Business Advisor, 24 mai. 2013. Disponível em: <http://smallbusiness.yahoo.com/advisor/bitcoin-next-generation-online-payments-213922448--finance.html>. Acesso em: 11 dez. 2013.

17 YUNUS, Muhammad. Banker to the Poor: Micro-lending and the Battle against World Poverty. New York: Public Affairs, 2003.

18 PINAR ARDIC, HEIMANN e MYLENKO. Access to Financial Services and the Financial Inclusion Agenda around the World. Policy Research Working Paper, World Bank Financial and Private Sector Development Consultative Group to Assist the Poor, 2011. Disponível em: <https://openknowledge.worldbank.org/bitstream/handle/10986/3310/WPS5537.pdf>. Acesso em: 12 dez. 2013.

19 FONG, Jeff. How Bitcoin Could Help the World's Poorest People. PolicyMic, mai. 2013. Disponível em: <http://www.policymic.com/articles/41561/bitcoin-price-2013-how-bitcoin-could-help-the-world-s-poorest-people>. Acesso em: 12 dez. 2013.

20 SPAVEN, Emily. Kipochi launches M-Pesa Integrated Bitcoin Wallet in Africa. CoinDesk, 19 jul. 2013. Disponível em: <http://www.coindesk.com/kipochi-launches-m-pesa-integrated-bitcoin-wallet-in-africa/>. Acesso em 12 dez. 2013.

21 MATONIS, Jon. Bitcoin's Promise in Argentina. Forbes, 27 abr. 2013. Disponível em: <http://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/>. Acesso em: 12 dez. 2013.

22 RUSSO, Camila. Bitcoin Dreams Endure to Savers Crushed by CPI: Argentina Credit. Bloomberg, 16 abr. 2013. Disponível em: <http://www.bloomberg.com/news/2013-04-16/bitcoin-dreams-endure-to-savers-crushed-by-cpi-argentina-credit.html>. Acesso em: 12 dez. 2013.

23 BRITO, Jerry. The Top 3 Things I Learned at the Bitcoin Conference. Reason, 20 mai. 2013. Disponível em: <http://reason.com/archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoi>. Acesso em: 12 dez. 2013.

24 HEARN, Mike. Bitcoin 2012 London: Mike Hearn. YouTube video, 28:19, publicado por "QueuePolitely," 27 set. 2012. Disponível em: <http://www.youtube.com/watch?v=mD4L7xDNCmA>. Acesso em: 13 dez. 2013. Propriedade inteligente (*smart property*) é um conceito para controlar propriedade de um item por meio de acordos feitos no *blockchain* do Bitcoin. A propriedade inteligente permite que as pessoas intercambiem propriedade de um produto ou serviço uma vez que uma condição é atingida usando a criptografia. Embora a propriedade inteligente seja ainda teórica, os mecanismos básicos já estão incorporados ao protocolo do Bitcoin. Ver Bitcoin wiki "Smart Property". Disponível em https://en.bitcoin.it/wiki/Smart_Property. Acesso em: 13 dez. 2013.

25 O financiamento coletivo (*crowdfunding*) consiste na obtenção de capital para iniciativas de interesse coletivo por meio da agregação de múltiplas fontes de financiamento, em geral, pessoas físicas interessadas na iniciativa. O termo é muitas vezes usado para descrever especificamente ações na internet com o objetivo de arrecadar dinheiro para artistas, jornalismo cidadão, pequenos negócios e startups, campanhas políticas, iniciativas de software livre, filantropia e ajuda a regiões atingidas por desastres, entre outras.

26 WILLETT, J. R. The Second Bitcoin Whitepaper, white paper, 2013. Disponível em: <https://sites.google.com/site/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf>. Acesso em: 13 dez. 2013.

27 KIRK, Jeremy. Could the Bitcoin Network Be Used as an Ultrasecure NotaryService? ComputerWorld, 23 mai. 2013. Disponível em: <http://www.computerworld.com/s/article/9239513/Could_the_Bitcoin_network_be_used_as_an_ultrasecure_notary_servi Acesso em: 13 dez. 2013.

28 WARREN, Jonathan. Bitmessage: A Peer-to-Peer Message Authentication and Delivery System, white paper, 27 nov. 2012. Disponível em: <https://bitmessage.org/bitmessage.pdf>. Acesso em: 13 dez. 2013.

29 MIERS, Ian et al. Zerocoin: Anonymous Distributed E-Cash from Bitcoin, working paper, the Johns Hopkins University Department of Computer Science,

Baltimore, MD, 2013. Disponível em: <http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf>. Acesso em: 13 dez. 2013.

30 LEE, Timothy B. An Illustrated History of Bitcoin Crashes, Forbes, 11 abr. 2013. Disponível em: <http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/>. Acesso em: 13 dez. 2013.

31 SALMON, Felix. The Bitcoin Bubble and the Future of Currency, Medium, 3 abr. 2013. Disponível em: <https://medium.com/money-banking/2b5ef79482cb>. Acesso em: 13 dez. 2013.

32 FARRELL, Maureen. Strategist Predicts End of Bitcoin, CNNMoney, 14 mai. 2013. Disponível em: <http://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/index.html>. Acesso em: 13 dez. 2013.

33 GURRI, Adam. Bitcoins, Free Banking, and the Optional Clause, Ümlaut, 6 mai. 2013. Disponível em: <http://theumlaut.com/2013/05/06/bitcoins-free-banking-and-the-optional-clause/>. Acesso em: 13 dez. 2013.

34 Hoje serviços como esse aceitam o risco inerente à volatilidade e ainda assim mantêm baixas taxas. Se esse modelo será sustentável no longo prazo, é algo inconclusivo.

35 A maioria dos desafios de segurança está relacionada aos serviços de carteiras e às casas de câmbio. O protocolo em si tem-se provado consideravelmente resiliente a hackers e riscos de segurança. O renomeado pesquisador de segurança Dan Kaminsky tentou, mas fracassou, hackear o protocolo Bitcoin em 2011. KAMINSKY, Dan. I Tried Hacking Bitcoin and I Failed, Business Insider, 12 abr. 2013. Disponível em: <http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4>. Acesso em: 13 dez. 2013.

36 O termo *malware* é proveniente do inglês *malicious software*; é um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano, alterações ou roubo de informações (confidenciais ou não).

37 COLDEWEY, Devin. $250,000 Worth of Bitcoins Stolen in Net Heist, NBC News, 5 set. 2012. Disponível em: <http://www.nbcnews.com/technology/250-000-worth-bitcoins-stolen-net-heist-980871>. Acesso em: 14 dez.2013.

38 KELLY, Meghan. Fool Me Once: Bitcoin Exchange Mt.Gox Falls after Third
DDoS Attack This Month, VentureBeat, 21 abr. 2013. Disponível em: <http://venturebeat.com/2013/04/21/mt-gox-ddos/>. Acesso em 14 dez. 2013.

39 Wikipedia "Deep Web". Disponível em http://en.wikipedia.org/wiki/Deep_Web. Acesso em: 30 jul. 2013.

40 O site Silk Road foi fechado pelas autoridades americanas no final de 2013, mas a associação do Bitcoin ao uso para fins criminosos é algo recorrente. Isso nos remete a um ponto fundamental: o Bitcoin é uma tecnologia e, portanto, não é boa nem má. É neutra. O crime está na ação do infrator, jamais na tecnologia empregada para tal. O Bitcoin, ou qualquer outra forma de dinheiro, pode ser usado para o bem ou para o mal. Além disso, a compra e venda de drogas, dependendo do país, já é algo normal e perfeitamente lícito. Isso quer dizer que a proibição das drogas é uma questão política que independe por completo do Bitcoin. Ademais, a experiência sugere que a guerra às drogas é muito mais nefasta do que qualquer consequência derivada de seu uso por cidadãos honestos.

41 CHRISTIN, Nicolas. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace, Carnegie Mellon CyLab Technical Reports: CMU-CyLab-12-018, 30 jul. 2012 (atualizado em 28 Nov. 2012). Disponível em: <http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf>. Acesso em: 14 dez. 2013.

42 BRITO, Jerry. National Review Gets Bitcoin Very Wrong, Technology Liberation Front, 20 jun. 2013. Disponível em: <http://techliberation.com/2013/06/20/national-review-gets-bitcoin-very-wrong/>. Acesso em: 14 dez. 2013.

43 WOLF, Brett. Senators Seek Crackdown on 'Bitcoin' Currency, Reuters, 8 jun. 2011. Disponível em: <http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608>. Acesso em: 14 dez. 2013.

44 Liberty Reserve Digital Money Service Forced Offline, BBC News—Technology, 27 mai. 2013. Disponível em: <http://www.bbc.co.uk/news/technology-22680297>. Acesso em: 14 dez. 2013.

45 SPARSHOTT, Jeffrey. Bitcoin Exchange Makes Apparent Move to Play by U.S. Money-Laundering Rules, Wall Street Journal, 28 jun. 2013. Disponível em: <http://online.wsj.com/article/SB10001424127887323873904578574000957464468.html>. Acesso em: 14 dez. 2013.

46 A exceção foi um caso, em julho de 2012, interpelado pela Comissão de Valores Mobiliários (CVM), ao impedir e multar um cidadão não registrado na autarquia de ofertar publicamente um veículo de investimento em bitcoins. Entretanto, não houve qualquer juízo de valor referente ao Bitcoin em si, apenas ao fato de que constituía uma oferta de investimento irregular em território nacional. Disponível em: <http://www.cvm.gov.br/port/infos/comunicado-deliberacao%20680.asp>.

A história e o contexto do Bitcoin

É COM A ANÁLISE DO CONTEXTO em que o Bitcoin surgiu que podemos entender a sua razão de ser. Ainda que possa ser considerada uma mera coincidência o fato de a moeda digital ter surgido em meio à maior crise financeira desde a Grande Depressão de 1930, não podemos deixar de notar o avanço do estado interventor, as medidas sem precedentes e arbitrárias das autoridades monetárias na primeira década do novo milênio e a constante perda de privacidade que cidadãos comuns vêm enfrentando em grande parte dos países desenvolvidos e emergentes.

Esses fatores são certamente responsáveis por parte do ímpeto da criação do Bitcoin. E, enquanto os reais motivos de seu surgimento podem ser apenas intuídos, não há dúvidas quanto ao que possibilitou o seu desenvolvimento: a era da computação, a revolução digital.

1. A Grande Crise Econômica do século XXI e a Perda de Privacidade Financeira

A quebra do banco Lehman Brothers, em setembro de 2008 – um dos grandes marcos da atual crise econômica e a maior falência da história dos Estados Unidos –, ocorreu há pouco mais de cinco anos. E, até hoje, seguimos sentindo as repercussões dessa grande crise.

No *mainstream* da ciência econômica, muito ainda se debate sobre as reais causas da débâcle financeira. A ganância, a desregulamentação do setor financeiro, os excessos dos bancos ou, simplesmente, o capitalismo, são todos elementos apontados como os causadores da crise. Mas é justamente o setor financeiro, aquele em que a intervenção dos governos é mais presente e marcante, seja em países desenvolvidos, seja em países em desenvolvimento. Assim, e como veremos adiante, o mais correto seria apontar o socialismo aplicado ao âmbito monetário como o real culpado e não o livre mercado.

O atual arranjo monetário[47] do Ocidente baseia-se em dois grandes pilares: 1) monopólio da emissão de moeda com leis de curso legal forçado[48]; e 2) banco central, responsável por organizar e controlar o sistema bancário. Em grande parte dos países, a tarefa de emissão de moeda é delegada pelo estado ao próprio banco central. É, portanto, patente a interferência governamental no âmbito monetário. Tal arranjo é a antítese de livre mercado; considerá-lo um exemplo de capitalismo exige uma boa dose de elasticidade intelectual.

Além disso, as moedas hoje emitidas pelos governos não têm lastro algum, senão a confiança dos governos. Ao longo de centenas de anos, o arranjo monetário desenvolveu-se de tal forma que não há mais vestígios de qualquer vínculo ao ouro ou à prata, ambos metais preciosos que serviram como dinheiro por milênios. O chamado padrão-ouro hoje não passa de um fato histórico com remotas possibilidades de retornar. E não porque não funcionava, mas porque impunha restrições ao ímpeto inflacionista dos governos. Quando estes emitiam moeda em demasia, acabavam testemunhando a fuga de ouro das fronteiras nacionais, sendo obrigados a depreciar a paridade cambial com o metal precioso.

Desde 1971, quando o então presidente Richard Nixon suspendeu a conversibilidade do dólar em ouro, vivemos na era do papel-moeda fiduciário, em que bancos centrais podem imprimir quantidades quase ilimitadas de dinheiro, salvo o risco de que os cidadãos percam toda a

confiança na moeda, recusando-se a usá-la em suas transações, como costuma ocorrer em episódios de hiperinflação[49].

A realidade é que recorrer à impressão de dinheiro é algo que os governos naturalmente fizeram ao longo da história para financiar seus déficits, para custear suas guerras ou para sustentar um estado perdulário incapaz de sobreviver apenas com os impostos cobrados da sociedade. O poder de imprimir dinheiro é tentador demais para não ser usado.

Mas, nos últimos cem anos, o mecanismo de impressão de dinheiro foi, de certa maneira, sofisticado. Antigamente, diluía-se o conteúdo do metal precioso de uma moeda, adicionando um metal de mais baixa qualidade. Na República de Weimar, as impressoras de papel-moeda operavam a todo o vapor 24 horas por dia. Atualmente, entretanto, o processo inflacionário é um pouco mais indireto e envolve não somente um Banco Central ou um órgão de governo imprimindo cédulas de dinheiro, mas também todo o sistema bancário.

Inflação é o aumento na quantidade de moeda em uma economia, e a eventual elevação dos preços é a consequência inevitável[50]. Mas, em uma economia moderna, a oferta de moeda não é composta apenas por cédulas e moedas de metal; os depósitos bancários também fazem parte da oferta monetária, uma vez que desempenham a mesma função que a moeda física. Ainda que não "existam" materialmente, os depósitos constituem parte da oferta monetária total. Assim, quando se emite moeda ou se criam depósitos bancários do nada, está ocorrendo inflação. E quanto maior a quantidade de dinheiro (oferta monetária) em uma economia, menor o poder de compra de cada unidade monetária. Ou, o seu corolário, mais caros se tornam os produtos e serviços.

Mas e como se multiplicam os depósitos bancários? Por meio de um mecanismo chamado reservas fracionárias. Em suma, significa que os bancos podem guardar nos seus cofres apenas uma fração do dinheiro que foi depositado e emprestar o restante ao público – daí o nome reservas fracionárias[51]. E o impacto desse arranjo no sistema financeiro é monumental, porque esse simples mecanismo concede aos bancos o poder de criar depósitos bancários por meio da expansão do crédito. E como depósitos bancários são considerados parte da massa monetária, os bancos criam moeda de fato – por isso, diz-se que os bancos são "criadores de moeda".

Além de aumentar a quantidade de moeda, a expansão do crédito pelo sistema bancário tem outro efeito nocivo na economia: a formação de ciclos econômicos[52]. Para que haja investimento, é preciso haver poupança. É o investimento que permite o acúmulo de capital, que, por sua vez, possibilita uma maior produtividade da economia. Mas sem poupança prévia não é possível investir. A expansão do crédito pelo sistema bancário sob um regime de reservas fracionárias permite que os bancos concedam empréstimos às empresas e indivíduos como se houvesse poupança disponível, quando, na verdade, isso não ocorreu. Logo, os empresários investem como se houvesse recursos disponíveis para levar a cabo seus empreendimentos, criando um auge econômico que contém as sementes de sua própria ruína. Cedo ou tarde, alguns investimentos não poderão ser concluídos (pois simplesmente não há recursos suficientes para que sejam completados lucrativamente), devendo ser liquidados o quanto antes. Esse é o momento da recessão, quando os excessos cometidos durante o *boom* precisam ser sanados para que a estrutura produtiva da economia retome o seu rumo de forma sustentável. Normalmente, o sinal que antecede um ciclo de auge é a redução artificial dos juros pelo banco central. Por meio da manipulação da taxa de juros, o banco central injeta moeda no sistema bancário, propiciando uma maior expansão do crédito.

As crises financeiras deste início de milênio são uma ilustração perfeita da teoria explicada, chamada de Teoria Austríaca dos Ciclos Econômicos. Foi a redução artificial dos juros pelo Federal Reserve que deu início ao *boom* no setor imobiliário americano logo após o estouro da bolha da internet, em 2001 – que, por sua vez, foi também precedida por um período de expansão monetária orquestrada pelo Federal Reserve. Anos de crédito farto e barato levaram a um superaquecimento da economia americana, em especial no setor da construção civil, inflando uma bolha imobiliária[53] de proporções catastróficas. E para piorar ainda mais o cenário, os principais bancos centrais do mundo seguiam a mesma receita de juros baixos para estimular a economia, formando bolhas imobiliárias em outros países também.

Cegados pelos baixos índices de inflação ao consumidor – enquanto os preços dos ativos imobiliários e financeiros disparavam –, os banqueiros centrais acreditavam piamente terem domado os ciclos econômicos; entráramos na chamada "Era da Grande Moderação". Infelizmente, a realidade logo veio à tona, e, com ela, todas as consequências perversas de um sistema monetário e bancário sujeito a mais absoluta intervenção.

Começando em 2007 com o imbróglio das hipotecas de alto risco (os *subprimes*) e o consequente "aperto da liquidez" (o *liquidiy crunch*), o setor financeiro logo congelou, os preços dos ativos despencaram – em especial os do setor imobiliário – e os grandes bancos do mundo ocidental viram-se praticamente insolventes.

No ano seguinte, a crise seria intensificada. Bancos e fundos de investimento buscavam desesperadamente sacar seus depósitos de instituições problemáticas. Era a versão moderna da velha corrida bancária. A interconectividade, a interdependência, a exposição mútua e os riscos de contraparte (o "*counterparty risk*") eram de tal magnitude e complexa mensuração que o sistema financeiro estava simplesmente à beira do colapso. Depois de seguidos resgates de bancos em dificuldades, fusões forçadas pelo Federal Reserve, acordos de "troca de liquidez" entre os principais bancos centrais do mundo ("*liquidity swap*"), legislações apressadas e desesperadas, o impensável ocorria: no dia 15 de setembro de 2008, um banco considerado "grande demais para quebrar" viria a falir. O Lehman Brothers entrava para a história como a maior falência dos Estados Unidos até então.

A queda do Lehman foi certamente um ponto de inflexão na crise. A partir daquele momento, os bancos centrais passaram a atuar com uma discricionariedade e arbitrariedade sem precedentes no mundo desenvolvido. A teoria econômica já não seria suficiente para justificar as medidas extraordinárias. Somente argumentos contrafatuais poderiam embasar o pleito dos banqueiros centrais: "Se adotarmos a medida X, o resultado pode ser ruim, mas se não fizermos nada, será ainda pior". A despeito de jamais terem previsto a crise de 2007/08, as autoridades monetárias ainda gozavam de enorme confiança perante os políticos e a opinião pública. E, dessa forma, carta branca era dada pelos governos aos bancos centrais. A cautela era preterida, e o caminho estava livre para o grande experimento monetário do novo milênio.

Desde setembro de 2008, o rol de medidas extremas e imprevistas empregadas pelas principais autoridades monetárias globais é realmente assombroso. Resgate de bancos, seguradoras e montadoras; nacionalização de instituições financeiras; trocas de liquidez entre bancos centrais; monetização de dívida soberana; redução das taxas de juros a zero – aliada à promessa de que nesse nível permanecerão por um bom tempo; e compras maciças de ativos financeiros e hipotecas, quase ilimitadas e sem fim predeterminado, os notórios "afrouxamentos quantitativos" (*quantitative easing*, ou QE). E qual foram os resultados desse experimento? Quadruplicar o balanço do Federal Reserve; incitar uma guerra cambial[54] mundial, em que bancos centrais historicamente prudentes – como o Banco Nacional da Suíça – passaram a

imprimir dinheiro desesperadamente, com o intuito de evitar uma apreciação abrupta de suas moedas; gerar imposição de controle de capitais, muitas vezes de forma velada; e reinflar os preços dos ativos financeiros (ações e bônus) e imobiliários, formando uma renovada bolha com potencial de destruição ainda maior.

Ao cidadão comum, resta assistir ao valor do seu dinheiro esvair-se, enquanto banqueiros centrais testam suas teorias, ora para salvar bancos, ora para resgatar governos quebrados, mas sempre sob o pretexto da inatingível estabilidade de preços. Na prática, a única estabilidade que existe é a da perda do poder de compra da moeda, e quanto a esta, a impotência da sociedade é absoluta.

E é precisamente este ponto que ficou claro na atual crise: o cidadão não tem controle algum sobre seu dinheiro[55] e está à mercê das arbitrariedades dos governos e de um sistema bancário cúmplice e conivente. Além do imenso poder na mão dos bancos centrais, a conduta destes – envoltas por enorme mistério, reuniões a portas fechadas, atas indecifráveis, critérios escusos, decisões intempestivas e autoritárias – causa ainda mais consternação e desconfiança, justamente o oposto do que buscam. O que, nos dias de hoje, é uma grande ironia, pois, enquanto as autoridades monetárias se esquivam do escrutínio público, exigem cada vez mais informações da sociedade, invadindo a privacidade financeira dos cidadãos.

Isso nos traz a outro desdobramento do paradigma atual que vivemos: a crescente perda de privacidade financeira, frequentemente justificada pela ameaça do terrorismo, real ou imaginário, a qual foi intensificada depois dos ataques às torres gêmeas do World Trade Center em setembro de 2001.

Sob a alegação de impedir o financiamento de atividades terroristas e lavagem de dinheiro, quem acaba sofrendo as consequências da supervisão e espionagem são os cidadãos de bem, que encontram cada vez mais dificuldade para proteger seus ativos e movê-los a qualquer jurisdição fora do alcance dos governos. Em países emergentes, cujo histórico de estritos controles de capitais é bastante notório, a falta de liberdade financeira não é novidade. Mas aos cidadãos de países de primeiro mundo, esse novo paradigma não é nada bem-vindo.

É provável que nenhum país desenvolvido tenha avançando tanto a agenda contra a privacidade financeira como os Estados Unidos. Seguidos acordos secretos[56] com a União Europeia, Suíça e outros portos financeiros tidos como seguros têm levado o cidadão americano a ser um cliente altamente indesejado, quando não rejeitado em primeira instância. Muitos bancos europeus e suíços têm preferido declinar esses clientes, para não ter que obedecer a todas as exigências do governo dos EUA, como aquelas impostas pela infame legislação FATCA[57] (*Foreign Account Tax Compliance Act*). Aprovada pelo Congresso em 2010, a FATCA simplesmente concede à Receita Federal dos EUA (*Internal Revenue Service*, ou IRS) o poder de violar o direito de privacidade de cidadãos que detenham investimentos ou contas bancárias no exterior. Além disso, recruta instituições financeiras como se agentes do IRS fossem, exigindo que monitorem e reportem clientes americanos, arcando com a totalidade dos custos para obedecer à legislação, sob pena de retaliações no caso de descumprimento.

Até mesmo a Suíça – cujo setor bancário tem sido historicamente um dos principais destinos para quem busca discrição e sigilo financeiro – tem sucumbido às demandas norte-americanas. As famosas contas numeradas – que permitem mais privacidade ao titular, por não ser necessário vincular seu nome à conta – tampouco estão livres dessa nova realidade. Pouco a pouco o governo dos EUA aperta o cerco à livre movimentação de capitais, pressionando governos ao redor do globo a adotar medidas prudenciais e cumprir as imposições das autoridades

americanas.

Este é o paradigma do atual milênio: crescente perda de privacidade financeira; autoridades monetárias centralizadas e opressivas que abusam do dinheiro isentas de qualquer responsabilidade; e bancos cúmplices e coadjuvantes no desvario monetário.

Entretanto, se por um lado o cenário é desalentador, por outro, o terreno é fértil para a busca de novas soluções. Coincidência ou não, um mês após a quebra do Lehman Brothers, era lançada a pedra fundamental de uma possível solução à instabilidade do sistema financeiro mundial.

2. O bloco gênese

Precisamente no dia 31 de outubro de 2008, Satoshi Nakamoto publicava o seu *paper*, "*Bitcoin: a Peer-to-Peer Electronic Cash System*[58]", em uma lista de discussão online de criptografia[59]. Baseado na simples ideia de um "dinheiro eletrônico totalmente descentralizado e *peer-to-peer*, sem a necessidade de um terceiro fiduciário", o sistema desenhado por Satoshi surgia como um novo experimento no campo financeiro e bancário.

A ideia em si não era nova. Na verdade ela já havia sido brevemente explicitada por Wei Dai, membro da lista de discussão *cypherpunk*[60], em 1998. Em seu texto, Wei Dai expunha as principais características do protocolo de uma criptomoeda e como ela poderia funcionar na prática[61]. O próprio Satoshi, reconhecendo as origens conceituais do Bitcoin, cita o texto de Wei Dai como a primeira referência em seu *paper.*

A um mero leigo no assunto, o *paper* de Satoshi pode ser pouco esclarecedor. Pode parecer um tanto técnico e pouco conceitual. E quase nada revela sobre as razões ideológicas por trás do Bitcoin. Por sorte, após tornar pública a ideia do Bitcoin, Satoshi pôs-se a responder as perguntas dos demais participantes da lista de discussões, esclarecendo desde temas técnicos e conceituais até questões políticas e econômicas; é exatamente lá que encontramos os indícios do pensamento político-filosófico de Satoshi.

Várias postagens suas ilustram a visão de mundo e o conhecimento econômico do criador do Bitcoin. Por exemplo, quando confrontado com a afirmação de que "não seria encontrada uma solução aos problemas políticos na criptografia", Satoshi concordou, mas ressaltou que "podemos vencer uma grande batalha na corrida armamentista e ganhar um novo território de liberdade por vários anos. Governos são bons em cortar a cabeça de redes centralmente controladas, como o Napster, mas redes puramente P2P, como Gnutella e Tor, parecem seguir em frente inabaladas[62]".

Em uma postagem posterior, um membro do grupo conclui que o protocolo do Bitcoin garante uma inflação de 35%, ao que Satoshi o corrige, atentando para a regra de que a oferta de bitcoins ao longo do tempo é sabida com antecedência por todos os participantes. "Se a oferta de moeda aumenta à mesma taxa de crescimento de pessoas que a usam, os preços permanecem estáveis", destaca Satoshi, concluindo que "se ela não cresce tão rápido quanto a demanda, haverá deflação, e os primeiros detentores da moeda verão seu valor aumentar"[63].

Mas talvez o vestígio mais interessante sobre a visão crítica de Satoshi acerca dos sistemas monetário e bancário vigentes esteja gravado justamente no bloco gênese[64], o primeiro bloco do

blockchain. Às 18h15 do dia 3 de janeiro de 2009, nascia oficialmente o Bitcoin, com a primeira transação de sua história, transmitida à rede por Satoshi, registrada no bloco gênese e acompanhada da seguinte mensagem:

THE TIMES 03/JAN/2009 CHANCELLOR ON BRINK OF SECOND BAILOUT FOR BANKS

A alusão à manchete do jornal britânico *The Times* daquele dia não é acidental. É, na verdade, um claro indicativo da visão crítica de Satoshi sobre o sistema bancário e a desordem financeira reinante. Nesse contexto, o projeto Bitcoin vinha a ser uma tentativa de resposta à instabilidade financeira causada por décadas de monopólio estatal da moeda e por um sistema bancário de reservas fracionárias.

Poucos dias após a transmissão do bloco gênese, era disponibilizado aberta e gratuitamente para *download* o cliente Bitcoin v0.1. Era o início do grande experimento monetário e bancário do novo milênio.

3. O que possibilitou a criação do Bitcoin

Os motivos fundamentais que impulsionaram a criação do Bitcoin são, portanto, evidentes: um sistema financeiro instável e com elevado nível de intervenção estatal e a crescente perda de privacidade financeira. Mas esse estado de coisas não é novidade. A intervenção dos governos no âmbito monetário é milenar, assim como a cumplicidade e conivência do sistema bancário. A diferença entre o sistema financeiro mundial atual e o de cem anos atrás é meramente de grau; na sua essência, a intervenção estatal prevalece tanto hoje como no início do século XX. Por que então algo como o Bitcoin não surgiu antes? Por que precisamos assistir ao sistema financeiro mundial tornar-se tão vulnerável, a ponto de quase testemunharmos o seu mais absoluto colapso em 2008? Simplesmente porque, antes, uma tecnologia como a internet não estava disponível e madura como hoje está; de fato, a rede mundial de computadores foi o que viabilizou a criação do Bitcoin. A era da informação revolucionou diversos aspectos da cooperação social, e não poderia ser diferente com uma das instituições mais importantes para o convívio em sociedade, o dinheiro.

Aparentemente surgido do nada, o Bitcoin é, em realidade, resultado de mais de duas décadas de intensa pesquisa e desenvolvimento por pesquisadores praticamente anônimos. No seu âmago, o sistema é um avanço revolucionário em ciência da computação, cujo desenvolvimento foi possibilitado por 20 anos de pesquisa em moedas criptográficas e 40 anos de pesquisa em criptografia por milhares de pesquisadores ao redor do mundo[65].

Mas para entendermos melhor como a ciência da computação e a internet possibilitaram a criação do experimento Bitcoin, é preciso ir mais além e compreender as principais tecnologias intrínsecas ao sistema. Basicamente, o Bitcoin é a junção de duas tecnologias: a distribuição de um banco de dados por meio de uma rede *peer-to-peer* e a criptografia. A primeira foi somente possível com o advento da internet. Já a segunda é bastante antiga, mas seu potencial não poderia ter sido devidamente explorado antes da era da computação.

Ao contrário das redes usuais, em que há um servidor central e os computadores (clientes ou nós, *nodes*, em inglês) se conectam a ele, uma rede *peer-to-peer* não possui um servidor centralizado. Nessa arquitetura de redes, cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor – cada um dos nós é igual aos demais (*peer* traduz-se como “par” ou “igual”) –, o que permite o compartilhamento de dados sem a necessidade de um servidor

central. Por esse motivo, uma rede *peer-to-peer* é considerada descentralizada, em que a força computacional é distribuída.

A ideia de redes distribuídas não é nova e vem se desenvolvendo desde 1960 nos Estados Unidos. Mas foi com o surgimento da internet que as redes *peer-to-peer* realmente ganharam terreno e notoriedade. No final da década de 90, com a criação do Napster[66], essas redes se tornaram ainda mais populares, atraindo dezenas de milhões de pessoas dedicadas a trocar arquivos de áudio entre si. Desde então, diversas variantes de redes descentralizadas surgiram[67], frequentemente visando a troca de arquivos digitais.

No caso do Bitcoin, a rede *peer-to-peer* desempenha uma função fundamental: a de garantir a distribuição do *blockchain* a todos os usuários, assegurando que todos os nós da rede detenham uma cópia atual e fidedigna do histórico de transações do Bitcoin a todo instante. Dessa forma, novas transações são transmitidas a todos os nós, registradas no log de transações único e compartilhado, tornando redundante a existência de um servidor central. Em um mundo pré-digital, seria simplesmente inconcebível levar a cabo tal logística.

A criptografia, entretanto, não é uma tecnologia nova. O estudo da arte de cifrar mensagens – em que somente o remetente e o destinatário têm acesso ao conteúdo – remonta aos tempos passados: os primeiros registros datam ao redor de 2.000 a.C., no Egito. Historicamente, a criptografia foi utilizada por estados em assuntos ligados às guerras e à diplomacia com objetivo de interceptar mensagens e desvendar comunicações encriptadas.

É na era da computação, contudo, que a criptografia atinge seu apogeu. Antes do século XX, a criptografia preocupava-se principalmente com padrões linguísticos e análise de mensagens, como a própria etimologia sugere (criptografia, do grego *kryptós*, “escondido”, e *gráphein*, “escrita”). Hoje em dia, a criptografia é também uma ramificação da matemática, e seu uso no mundo moderno se estende a uma gama de aplicações presentes no nosso cotidiano, sem que sequer a percebamos, como em sistemas de telecomunicações, comércio online ou para proteção de sites de bancos. A criptografia moderna permite a criação de comprovações matemáticas que oferecem um altíssimo nível de segurança.

Aplicada ao Bitcoin, a criptografia desempenha duas funções essenciais: a de impossibilitar que um usuário gaste os bitcoins da carteira de outro usuário (autenticação e veracidade das informações) e a de impedir que o *blockchain* seja violado e corrompido (integridade e segurança das informações, evita o gasto duplo). Além disso, a criptografia também pode ser usada para encriptar uma carteira, de modo que ela só possa ser utilizada com uma senha definida por seu proprietário.

Assim, a aliança das duas tecnologias, uma rede descentralizada e a criptografia moderna, torna realidade o que há alguns anos era absolutamente inconcebível na prática e que, há alguns séculos, nem mesmo em teoria poderia ter sido imaginado.

Rodapé

47 Para uma breve análise do colapso da ordem monetária do Ocidente, ver ROTHBARD, Murray N. O que o governo fez com o nosso dinheiro? São Paulo: Instituto Ludwig von Mises Brasil, 2013.
48 Leis de curso legal forçado (*legal tender laws* em inglês) são leis que obrigam os cidadãos em um determinado país a aceitar o dinheiro emitido pelo estado como meio de pagamento.
49 Os brasileiros viveram alguns episódios hiperinflacionários nas décadas de 1980 e 90.
50 Infelizmente, o conhecimento convencional define inflação como o aumento de preços, quando, na verdade, isso é a

consequência da inflação, e não inflação *per se*. Ver MISES, Ludwig von. A verdade sobre a inflação, Instituto Ludwig von Mises Brasil, 27 mai. 2008. Disponível em: <http://mises.org.br/Article.aspx?id=101>. Acesso em: 16 dez. 2013.

51 No Brasil, esse mecanismo se confunde com o conceito do “compulsório”, o qual é determinado pelo Banco Central. Atualmente, o percentual de “compulsório” para os depósitos à vista está estabelecido em 10%. Dessa forma, com um depósito hipotético de R$ 1.000, um banco pode expandir o crédito em R$ 9.000, criando do nada R$ 9.000 de depósitos à vista, pelo simples registro contábil (débito de R$ 9.000 em empréstimos contra crédito de R$ 9.000 em depósitos à vista).

52 MISES, Ludwig von. Ação Humana: Um Tratado de Economia. São Paulo: Instituto Ludwig von Mises Brasil, 2010.

53 Não foram as únicas razões, mas foi condição *sine qua non* à atividade econômica insustentável. Para mais detalhes, ver WOODS Jr., Thomas E. Meltdown. Washington: Regnery Publishing, 2009.

54 RICKARDS, James. Currency Wars. New York: Penguin, 2011.

55 Talvez no Brasil isso fosse diferente, mas no exterior é inédito.

56 Another Loss of Personal & Financial Privacy, The Sovereign Society, 13 jul. 2010. Disponível em: <http://sovereignsociety.com/2010/07/13/another-loss-of-personal-financial-privacy/>. Acesso em: 20 dez. 2013.

57 Foreign Account Tax Compliance Act, Internal Revenue Service, 2010. Disponível em: <http://www.irs.gov/Businesses/Corporations/Foreign-Account-Tax-Compliance-Act-%28FATCA%29>. Acesso em: 20 dez. 2013.

58 NAKAMOTO, Satoshi. Bitcoin: a Peer-to-Peer Electronic Cash System, 2008. Disponível em: <http://article.gmane.org/gmane.comp.encryption.general/12588/>. Acesso em: 20 dez. 2013.

59 Recomento fortemente ler na íntegra as trocas de mensagens entre os participantes e o próprio Satoshi Nakamoto após a publicação de seu *paper.* Disponível em: <http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>. Acesso em: 20 dez. 2013.

60 Disponível em: <http://en.wikipedia.org/wiki/Cypherpunk>. Acesso em: 21 dez. 2013.

61 Nas palavras de Wei Dai, uma criptomoeda teria impactos extraordinários: “Eu estou fascinado com a cripto-anarchia do Tim May [membro fundador da lista de discussão *Cypherpunk*]. Ao contrário das comunidades tradicionalmente associadas à palavra ‘anarquia’, em uma cripto-anarquia o governo não é temporariamente destruído, mas permanentemente proibido e permanentemente desnecessário. É uma comunidade em que a ameaça de violência é impotente porque é impossível, e a violência é impossível porque os participantes não podem ser vinculados aos seus nomes verdadeiros ou às localidades físicas... Até agora não está claro, até mesmo teoricamente, como tal comunidade poderia operar. Uma comunidade é definida pela cooperação de seus participantes e cooperação eficiente requer um meio de troca (dinheiro) e uma forma de fazer cumprir contratos. Tradicionalmente esses serviços têm sido providos pelo governo ou por instituições patrocinadas pelo governo e somente a entidades jurídicas. Neste artigo eu descrevo um protocolo pelo qual esses serviços podem ser providos para e por entidades não rastreáveis... O protocolo proposto neste artigo permite que entidades pseudônimas não rastreáveis cooperem umas com as outras mais eficientemente, por meio da provisão de um meio de troca e um método de fazer cumprir contratos. Provavelmente o protocolo pode ser aprimorado, mas espero que isso seja um passo à frente do sentido de tornar a cripto-anarquia uma possibilidade prática e teórica”. Disponível em: <http://www.weidai.com/bmoney.txt>. Acesso em: 21 dez. 2013.

62 Disponível em: <http://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html>. Acesso em: 21 dez. 2013.

63 Disponível em: <http://www.mail-archive.com/cryptography@metzdowd.com/msg09979.html>. Acesso em: 21 dez. 2013. Aqui Satoshi emprega o conceito de inflação e deflação no sentido de aumento ou redução dos preços, e não no sentido de aumento ou redução da oferta monetária (conforme o conceito da Escola Austríaca de Economia).

64 Disponível em: <https://en.bitcoin.it/wiki/Genesis_block>. Acesso em: 21 dez. 2013.

65 Ver artigo de Marc Andreessen, sócio-fundador da empresa de *venture capital* Andreessen Horowitz, investidora de algumas empresas dedicadas ao desenvolvimento do Bitcoin, Why Bitcoin Matters, 22 jan. 2014. Disponível em: <http://blog.pmarca.com/2014/01/22/why-bitcoin-matters/>. Acesso em: 26 jan. 2014.

66 Em realidade, o Napster era uma rede semicentralizada, pois ainda que os computadores intercambiassem arquivos entre si, de forma *peer-to-peer*, os usuários conectavam-se a um servidor central – que continha os dados dos usuários, bem como o endereço de suas pastas e arquivos de música –, para a busca de arquivos. Devido a sua natureza semicentralizada, o Napster foi facilmente encerrado pelas autoridades americanas em 2001.

67 Por exemplo, a Gnutella e o BitTorrent, ambos ativos e operantes.

O que a teoria econômica tem a dizer sobre o Bitcoin

"O maior erro que pode ser feito na investigação econômica é o de fixar a atenção a meras aparências e, assim, fracassar em perceber a diferença fundamental entre coisas cujos exteriores apenas são similares, ou de discriminar entre duas coisas fundamentalmente similares cujos exteriores apenas são distintos."

Ludwig von Mises, *The Theory of Money and Credit*

O EXPERIMENTO BITCOIN É, no mínimo, intrigante. Ao economista, ele impõe algumas complicações que, à primeira vista, podem levar muitos estudiosos a uma apressada rejeição – deslize este que o presente autor confessa abertamente ter cometido. Boa parte do ceticismo em relação à moeda digital reside na complexidade tecnológica intrínseca ao Bitcoin, o que intimida muitos economistas – especialmente os de idade mais avançada – e impede uma sincera apreciação do fenômeno. Outra possível razão – relacionada ao que foi explicado no capítulo anterior – é que a existência de um sistema como o Bitcoin era simplesmente inconcebível na prática e quase impossível de imaginar em teoria. A muitos economistas, a própria acepção dessa realidade pode ser um desafio. A outros, a precipitada classificação de bolha é suficiente para ignorar a moeda digital.

Independentemente da justificativa, o fato é que Bitcoin existe. E uma vez que a realidade está dada – o Bitcoin foi concebido e lançado, evolui e perdura –, qual deve ser a postura do economista? Prender-se cegamente às suas teorias, negando a realidade? Creio que não, outro caminho é possível. Com honestidade e humildade, é preciso dar um passo atrás, revisitar a teoria econômica, buscando interpretar a realidade, observando os fenômenos e aplicando o conhecimento acumulado até o presente. Durante o processo, é possível que velhas teorias precisem ser revistas ou refinadas. E, como alerta Mises, sempre procurando distinguir as meras aparências da essência das coisas.

Mas qual teoria monetária deve guiar a análise do Bitcoin? Mises classifica as teorias monetárias a partir da dicotomia *cataláctica* e *acataláctica*[68]. A teoria monetária cataláctica explica os fenômenos monetários por meio das leis das trocas de mercado. É por meio dos intercâmbios de mercado que o dinheiro surge, e é pela lei da oferta e demanda que seu valor ou poder de compra é determinado. Uma teoria do valor do dinheiro precisa incorporar esse enfoque, o que não garante que ela será correta. Mas uma teoria monetária que ignora a perspectiva cataláctica jamais será satisfatória[69].

Dentre as teorias monetárias acatalácticas, a Teoria Estatal da Moeda, de Georg Friedrich Knapp, é a mais proeminente. Segundo ela, o valor da moeda é derivado de decreto governamental. Seu poder de compra é estabelecido por lei – *valor impositus*: o valor da moeda depende da autoridade estatal. À luz da Teoria Estatal da Moeda, a análise do Bitcoin acabaria sem nem sequer começar; o estado não reconhece Bitcoin como moeda e, portanto, a moeda não tem valor algum. Logo, não nos pode servir como ferramental teórico para analisar o fenômeno. A teoria nada tem a dizer sobre Bitcoin. E isso se deve ao fato não de ser uma teoria monetária ruim, mas sim, em realidade, de *não ser uma teoria monetária sequer*[70].

Assim, e como é evidente, é a partir da teoria monetária cataláctica de Mises que basearemos

nosso estudo da moeda digital. Entretanto, antes de iniciarmos a análise econômica, é preciso definir com precisão alguns termos e conceitos, para que não haja ambiguidade e que o entendimento seja o mais claro possível.

Meio de troca é um bem econômico utilizado nas trocas indiretas que soluciona o problema da dupla coincidência de desejos das trocas diretas, ou escambo. O padeiro quer leite, enquanto o leiteiro quer um sapato. Como resolver o problema? O padeiro também tem sal e sabe que o sapateiro e outros produtores também o demandam. Logo, o leiteiro, em troca de seu leite, aceita o sal, não para consumi-lo, mas para trocá-lo no futuro pelo sapato do sapateiro. À medida que mais indivíduos passam a usar o sal nas trocas indiretas, a mercadoria torna-se, consequentemente, um meio de troca.

Eventualmente, um meio de troca ganha mais mercado, ampliando sua liquidez, emergindo como o meio de troca universalmente aceito, tornando-se, então, *dinheiro*.

Frequentemente, o termo *moeda* e *dinheiro* confundem-se, especialmente na língua portuguesa. Moeda pode ser o dinheiro ou o padrão monetário usado em determinado país (como o dólar nos Estados Unidos e o real no Brasil). Neste último sentido, o termo equivale à palavra inglesa *currency*. Moeda também são as moedas físicas usadas como dinheiro, sejam elas feitas de cobre, ouro ou qualquer outro material. Dinheiro, em português coloquial, engloba, sobretudo, os conceitos de papel-moeda e as moedas metálicas que usamos nas trocas do dia a dia (“pagamento com cheque ou em dinheiro?”). Salvo expressamente indicado em contrário, utilizaremos o termo *dinheiro* no sentido de meio de troca universalmente aceito, ora intercambiando, sem prejuízo de entendimento, com o termo *moeda*.

Juridicamente, moeda é o meio de pagamento definido em lei pelo estado. Ao economista, a terminologia jurídica pouco interessa. E por essa razão, devem-se descartar as definições de moeda – às quais muitos economistas se apegam – que a qualificam como um símbolo da nação, de identidade nacional, etc. Essa noção deriva da visão do meio de troca como uma criatura do estado e que a ele pertence. A moeda não é propriedade do soberano, nem de nenhum governo. Embora tenha estado sob controle de governos em grande parte da história, sua origem é cataláctica, independentemente das disposições legais em certo tempo e lugar.

Ao fim deste capítulo, retomaremos a definição de moeda, buscando aportar algumas matizações a essa questão fundamental, refinando assim nosso próprio entendimento sobre a instituição do dinheiro em geral e o Bitcoin em particular.

Feito esse preâmbulo, podemos agora dar início a essa empreitada para compreender o fenômeno e como ele pode impactar o mundo em que vivemos.

1. O nascimento do dinheiro

Quando iniciamos a análise do Bitcoin, as dúvidas abundam. A moeda digital seria mesmo considerada dinheiro? A inovação não seria na verdade um mero sistema de pagamentos ou de transferência de fundos? Pode uma unidade de bitcoin, algo que inexiste no mundo físico, ser considerado um bem? Há valor intrínseco em uma moeda virtual? Qual o lastro do Bitcoin? Estaríamos revivendo a bolha das Tulipas na versão digital?

Para responder satisfatoriamente essas e outras questões relacionadas ao fenômeno Bitcoin, nosso ponto de partida da análise econômica deve ser sempre o mesmo: o estudo da ação humana, ou praxeologia. Curiosamente, a praxeologia parece ser a melhor ferramenta para

analisar o mundo virtual do Bitcoin e sua relação com as ações dos indivíduos, porque ela “lida não com o mundo exterior, mas com a conduta do homem em relação ao mundo exterior[71]”. A intangibilidade do Bitcoin, ao economista, não deveria impor uma complexidade adicional, pois a economia “não trata de coisas ou de objetos materiais tangíveis; trata de homens, de suas apreciações e das ações que daí derivam[72]”.

O homem atua para atingir seus objetivos, empregando meios considerados por ele próprio como adequados à consecução do fim desejado. Após o início da operação do software Bitcoin v0.1, Satoshi gastou os primeiros bitcoins em uma transação com Hal Finney no dia 12 de janeiro de 2009[73]. Visando testar o funcionamento do sistema (o fim), Satoshi transferiu seus bitcoins (meio) a Hal Finney. Se esse realmente foi o fim almejado por Satoshi, só podemos especular. Identificar o fim pretendido da ação não é o objetivo do estudo econômico. A partir do axioma da ação humana, sabemos que o homem age utilizando-se de meios para atingir seus fins, e isso é tudo o que precisamos saber. No caso de Satoshi, temos o registro histórico de uma ação – o primeiro gasto de bitcoins – em que bitcoins foram usados como meio para a consecução do fim desejado, independentemente de qual seja ele.

À medida que o Bitcoin foi progredindo, outros usuários passaram a utilizar bitcoins para a consecução de seus objetivos – dos mais variados, como o *geek* que quer ostentar as maravilhas de uma criptografia; o sujeito que compra bitcoins como forma de protesto ao *status quo*; ou os entusiastas envolvidos no projeto Bitcoin que buscam testar a nova ferramenta. Como dito acima, o essencial não é identificar com precisão o objetivo de cada indivíduo, mas sim ressaltar o registro histórico de que indivíduos atuaram empregando bitcoins como meio para a consecução de um fim.

Ainda que o fim último do projeto Bitcoin seja torná-lo um meio de troca totalmente eletrônico, naquele instante, bem no início de sua vida, bitcoins eram adquiridos não para serem empregados como um meio de troca, e sim para o próprio consumo direto, de modo a atingir o fim pretendido; e esse é precisamente o ponto de partida para que qualquer bem venha a tornar-se um meio de troca e, eventualmente, dinheiro, o meio de troca universalmente aceito. É preciso que o bem em questão proporcione um valor de uso – seja ele qual for – antes de ser utilizado como meio de troca. No início de 2009, aos olhos dos seus compradores, bitcoins eram simplesmente mercadorias virtuais, bens econômicos, e nada mais além disso. *A esses compradores*, bitcoins supriam uma necessidade e eram úteis, isto é, detinham uma utilidade. Por que grifar “a esses compradores”? Porque a utilidade aqui definida é algo subjetivo, é percebida pelo próprio ator – nesse caso, os adquirentes de bitcoins – e não pode ser observada por um terceiro.

É importante aprofundarmo-nos, neste momento, no conceito de utilidade, pois muitas das críticas ao Bitcoin se baseiam em uma errônea, ou incompleta, noção de utilidade. Mises, em *Ação Humana*, explica que:

> *Utilidade* significa simplesmente relação causal para a redução de algum desconforto. O agente homem supõe que os serviços que um determinado bem podem produzir irão aumentar o seu bem estar e a isto denomina utilidade do bem em questão. Para a praxeologia, o termo utilidade é equivalente à importância atribuída a alguma coisa em razão de sua suposta capacidade de reduzir o desconforto. A noção praxeológica de utilidade (valor de uso subjetivo segundo a terminologia dos primeiros economistas da Escola Austríaca) deve ser claramente diferenciada da noção tecnológica de utilidade (valor de uso objetivo, segundo a terminologia dos mesmos economistas). Valor de uso

objetivo é a relação entre uma coisa e o efeito que a mesma pode produzir. É ao valor de uso objetivo que nos referimos ao empregar termos tais como ‘valor calórico’ ou ‘potência calorífica’ do carvão. *O valor de uso subjetivo não coincide necessariamente com o valor de uso objetivo.*[74] (ênfase do presente autor).

Qual o seria valor de uso objetivo de uma unidade de bitcoin? Qual é a utilidade *tecnológica* de um bitcoin? Talvez a principal resida no fato de que somente bitcoins podem ser usados na rede Bitcoin. Não é possível transferir dólares pelo *blockchain*, mas bitcoins, sim. Essa propriedade *intrínseca* de um bitcoin é algo extremamente útil. Além disso, um bitcoin pode ser usado para designar e certificar *propriedade de um bem*. Neste primeiro momento, os próprios bitcoins são o bem em questão. À medida que a rede se desenvolva, é plenamente possível que outras utilidades e aplicações venham a ser descobertas ou criadas pelo homem[75].

Mas qual seria o valor de uso subjetivo de um bitcoin? Somente cada indivíduo pode determinar. O que o economista pode inferir é que bitcoins *foram* e *têm sido* valorados pelos indivíduos que os adquiriram e os utilizam independentemente de qual seja o uso pretendido.

Em *Theorie des Geldes und Umlaufsmittel*[76] (Teoria do Dinheiro e da Moeda Fiduciária), sua primeira grande obra, Ludwig von Mises expõe o famoso teorema da regressão para analisar e compreender a origem e o valor do dinheiro. Segundo esse teorema, é impossível qualquer tipo de dinheiro surgir já sendo um imediato meio de troca; um bem só pode alcançar o status de meio de troca se, antes de ser utilizado como tal, ele já tiver obtido algum valor como mercadoria. Qualquer que seja o meio de troca, ele precisa antes ter tido algum uso como mercadoria, para só então passar a funcionar como meio de troca. É preciso que haja um valor de uso prévio ao valor de meio de troca.

No caso do ouro e da prata, sabemos que foram escolhidos pela humanidade como o dinheiro por excelência ao longo de centenas de anos por meio de milhões de intercâmbios no mercado. Mas seria impossível datar precisamente quando o ouro surgiu como mercadoria, quando passou a ser utilizado como meio de troca e quando preponderou como o bem mais líquido ou mais “vendável” *(marketable),* tornando-se, por fim, o meio de troca universalmente aceito, ou, simplesmente, dinheiro.

No caso de Bitcoin, temos a data exata: a moeda digital nasceu no dia 3 de janeiro de 2009. Alguns meses depois, passou a ser consumida, ou adquirida, não para ser usada como meio de troca – afinal de contas, pouquíssimos indivíduos nem sequer o conheciam –, mas sim para satisfazer alguma necessidade individual, ou seja, certo valor de uso estava presente. E não é imprescindível identificarmos com exatidão qual necessidade ou objetivo levou os primeiros compradores de bitcoin a trocar alguns dólares por uma unidade bitcoin (1 BTC). O que importa não é o *porquê*, mas sim o fato de que houve demanda real e bitcoins foram adquiridos e preços foram formados na busca por essa mercadoria. Nesse sentido, o nascimento do Bitcoin em nada contraria o teorema da regressão de Mises, pois tudo o que precisamos demonstrar é que “*valor de uso esteve presente em algum momento, bem no início e dentro da escala de valores das pessoas envolvidas em criar e negociar com a mercadoria*[77]”.

Dentre os economistas da Escola Austríaca, essa é uma questão contenciosa, uma vez que vários alegam que o Bitcoin contraria o *teorema da regressão*. Como explicado acima, tal alegação não se sustenta. Mas é essencial, enquanto economistas, desenvolvermos o argumento com mais profundidade. E para isso, é preciso deixar claro o que o teorema da regressão *não* afirma. Por exemplo, o teorema não afirma que, a fim de uma mercadoria tornar-se meio de

troca, é preciso um *amplo* e *facilmente identificado* valor de uso objetivo ou utilidade tecnológica. O teorema também não define, nem elenca, as propriedades intrínsecas necessárias para que um bem seja empregado pelo mercado como um eventual meio de troca. Também não é estabelecido com qual *intensidade* nem *por quanto tempo* o bem deva apresentar algum valor de uso reconhecido pelos indivíduos. O teorema, contudo, afirma ser necessária a presença de *algum* valor de uso *subjetivo* prévio ao aparecimento do valor de troca, mesmo que um terceiro não consiga observá-lo. Antes de ser empregada como um meio de troca, a mercadoria precisa ser valorada *pelo indivíduo* devido às suas propriedades intrínsecas – *sejam elas quais forem* – e ao efeito que estas podem ter, segundo *julgamento do próprio indivíduo*.

Ao expor o teorema, Mises usou o *exemplo* do ouro como a mercadoria que, escolhida pelo mercado, passou a ser valorada não somente por suas qualidades intrínsecas (valor de uso objetivo), mas também como um meio de troca (valor de troca). O ouro, portanto, serviu como ilustração histórica, não como comprovação teórica do teorema da regressão.

Imaginando-se o surgimento do ouro no mercado, poderíamos traçar alguns paralelos entre o que ocorreu então e as críticas atuais contra o Bitcoin. Por exemplo, quando o metal foi descoberto, qual era o seu valor de uso objetivo? Qual a utilidade de um metal cujas propriedades físico-químicas não permitiam que ele servisse como alimento ao homem? Nem tampouco pudesse servir para prender fogo?[78] Agora seu valor de uso *subjetivo* está amplamente documentado. Na maior parte dos exemplos históricos, o ouro serviu basicamente como adorno, como enfeite à vestimenta ou a casas, templos, etc. Seu uso industrial, como o conhecemos atualmente, foi somente possibilitado após alguns milênios de progresso econômico. Quando o metal surgiu, é plenamente possível que ele apresentasse *pouquíssimas* aplicações; era muito pouco útil sob a perspectiva de seu valor de uso objetivo. Mas isso não o impediu de ser empregado cada vez mais como um meio de troca, passando a ser cada vez mais valorado como tal do que apenas como uma mercadoria que pouco valor de uso parecia proporcionar. Quando, por fim, o ouro preponderou como o meio de troca mais líquido (a moeda), seu valor de uso passou a coincidir com o valor de troca, isto é, sua utilidade residia principalmente no seu emprego como meio de troca, e não como adorno. A partir desse instante, já não é mais necessário que o bem usado como moeda apresente algum outro uso além de meio de troca. Após a transição de mercadoria para meio de troca universalmente aceito, seu valor pode depender exclusivamente de seu uso como dinheiro.

É precisamente esse o caminho percorrido pelo Bitcoin. De uma mercadoria virtual – com pouco valor de uso objetivo identificado, mas algum valor de uso subjetivo, conforme percebido por alguns indivíduos –, um bitcoin passou a ser empregado como meio de troca, embora muito menos líquido do que as moedas que estamos acostumados a utilizar.

Mas quando exatamente o Bitcoin virou meio de troca? A primeira transação[79] de que se tem notícia se deu em maio de 2010, quando ‘laszlo’ trocou uma pizza por 10 mil BTC – em retrospecto, pode ter sido a pizza mais cara do mundo (10 mil BTC = 8,5 milhões de dólares, cotação de 23/11/13). Mises afirma que o teorema da regressão “não é meramente um conceito instrumental de teoria; é um fenômeno real de história econômica, que se faz aparente no momento em que a troca indireta começa”[80]. Dessa forma, o fenômeno Bitcoin nos fornece uma perfeita ilustração histórica da teoria monetária de Mises. O fato é que, desde então, bitcoins passaram a funcionar como meio de troca, de acordo com o seu objetivo fundamental. Estamos potencialmente testemunhando em “tempo real” o nascimento de uma moeda. E o que é mais extraordinário, com um vasto registro documental disponível para qualquer economista investigar. Não há incompatibilidade alguma entre o teorema da regressão de Mises e o

surgimento do Bitcoin. Ao contrário, este é a mais recente ilustração histórica daquele. O teorema é um enunciado praxeológico; cabe ao economista a função de aplicá-lo na interpretação de eventos históricos.

2. Escassez intangível e autêntica

"Os meios são, necessariamente, sempre escassos, isto é, insuficientes para alcançar todos os objetivos pretendidos pelo homem."[81] Chamamos de bens econômicos tudo aquilo que é empregado como meio no âmbito da ação humana. Bens econômicos estão sujeitos, portanto, à realidade da escassez; isso implica que um mesmo bem não pode ser usado como meio por mais de um indivíduo no mesmo instante. O meu uso de dado bem econômico exclui a possibilidade de uso dele por outros agentes.

No mundo material, dos bens físicos, essa relação é facilmente observada. Mas não somente objetos materiais podem ser empregados como meio na ação humana. "No nosso universo não existem meios; só existem coisas. Uma coisa só se torna um meio quando a razão humana percebe a possibilidade de empregá-la para atingir um determinado fim e realmente a emprega com este propósito."[82] A possibilidade de empregar um bem como meio reside nas propriedades deste, as quais não estão restritas a um sentido puramente físico. Corpóreo ou não, um bem pode ser empregado como meio quando é capaz de oferecer serviços úteis à consecução de um fim.

Mas como encaixar bens digitais – como o Bitcoin – nesse contexto? Bens digitais não são quase infinitamente reproduzíveis, portanto, não escassos? De fato, a era digital levou o economista a confrontar problemas antes pouco explorados ou até mesmo pouco compreendidos. Um refinamento sobre a escassez dos bens econômicos é fundamental[83].

Tucker e Kinsella elucidam que um objeto pode 1) ser um bem econômico (no sentido de meio na estrutura da ação humana) e escasso, como um sapato, uma caixa de suco, etc.; 2) não ser um bem econômico, mas escasso, como uma lesma ou uma sopa com veneno; 3) ser um bem econômico e não escasso, como uma receita de bolo, uma ideia, etc.; e 4) não ser um bem econômico nem escasso, como uma ideia ruim, um som horrível, etc. O advento da computação, e com ela, da mídia digital, expandiu a quantidade de objetos que poderiam ser classificados como bens econômicos não escassos. Um arquivo digital (como uma planilha em Excel, um arquivo de texto, arquivos de áudio MP3 ou vídeo MP4, etc.) pode ser reproduzido inúmeras vezes sem que a cópia original seja de qualquer forma prejudicada. Isto é, o proprietário do arquivo original pode utilizá-lo da forma que bem entender simultaneamente com os detentores das diversas cópias. Resumidamente, "um bem não escasso é um bem copiável enquanto o original permanece intacto e é utilizável por múltiplos atores simultaneamente e sem interferência mútua"[84].

Aplicando essas definições ao caso do Bitcoin, verificamos que a questão é distinta. Um bitcoin pode existir somente em uma carteira em dado momento devido ao protocolo do sistema que registra todas as transações no *blockchain* único e distribuído, que impede o gasto duplo. E é importante ressaltar que essa não é uma opção disponível do Bitcoin, mas sim uma característica integral e inseparável do software.

A tecnologia utilizada pelo protocolo do Bitcoin, uma rede *peer-to-peer*, aliada ao potencial da criptografia moderna faz com que uma unidade de bitcoin seja um bem econômico escasso, "um

bem *não* copiável enquanto o original permanece intacto e *não* utilizável por múltiplos atores simultaneamente e sem interferência mútua". Somente 21 milhões de unidades poderão ser criadas; ninguém pode gastar a mesma unidade diversas vezes e nenhuma unidade bitcoin pode ser gasta por vários usuários simultaneamente. Isso demonstra outra característica que define um bitcoin como um bem econômico: o poder do proprietário de controlar o seu bitcoin[85]. Somente o dono do bitcoin pode usar sua chave privada para dispor de seus bitcoins, transferindo-os a quem desejar.

O Bitcoin trouxe, portanto, escassez autêntica ao mundo dos bens digitais não escassos – uma escassez intangível e autêntica.

3. Moeda tangível e intangível

A criação do Bitcoin trouxe à tona algo que esteve presente com a humanidade por séculos, mas que talvez somente agora se tenha feito evidente: a intangibilidade do dinheiro que usamos. Mas para demonstrá-la, é preciso retornar à origem do dinheiro.

Os registros históricos documentam os mais diversos bens que desempenharam a função de meio de troca ao longo do tempo: tabaco, na Virgínia colonial; açúcar, nas Índias Ocidentais; sal, na Etiópia (na época, Abissínia); gado, na Grécia antiga; pregos, na Escócia; cobre, no Antigo Egito; além de grãos, rosários, chás, conchas e anzóis. Entretanto, ao longo dos séculos, duas mercadorias, o ouro e a prata, foram espontaneamente escolhidas como dinheiro na livre concorrência do mercado, desalojando todas as outras dessa função. A característica comum a todas essas mercadorias é a tangibilidade. Todos esses bens são objetos materiais que existem no mundo físico com propriedades químicas, físicas e até mesmo biológicas distintas.

Com o desenvolvimento e a intensificação da divisão do trabalho, o crescimento econômico exigiu um aperfeiçoamento do dinheiro utilizado nos intercâmbios no mercado. Surgiu então o serviço de custódia do ouro (ou qualquer outro metal monetário), no início provido pelos ourives e posteriormente pelos bancos, em que os depositantes recebiam certificados de armazenagem. Os certificados passaram, então, a circular como se o próprio metal fosse, facilitando o uso do dinheiro metálico. À medida que o uso do papel físico (o certificado ou cédula bancária, ou seja, um *substituto de dinheiro*) ampliou-se, o número de transações com o ouro de verdade diminuiu. Dessa forma, os bancos cresceram e ganharam gradativamente a confiança dos clientes, até o ponto de estes julgarem que era mais conveniente abrir mão de seu direito de receber a cédula bancária, e, em vez disso, manter sua titularidade na forma de contas que podiam ser movimentadas sob demanda, o que chamamos de depósitos bancários, ou contas-correntes.

Com esse arranjo, o cliente não precisa transferir a cédula a quem transaciona com ele; basta escrever uma ordem para que seu banco transfira uma porção da sua conta para outra pessoa. Essa ordem por escrito é chamada de cheque. Até este momento, a oferta monetária não sofreu aumento algum em decorrência do uso de substitutos monetários; as contas-correntes ou as cédulas bancárias são meros substitutos ao dinheiro físico depositado no banco, no caso, o ouro. Os substitutos de dinheiro têm 100% de lastro. Poderíamos dizer que toda a massa monetária se plasma em dinheiro material, tangível, isto é, em metal precioso depositado no banco, ainda que parte dele circule por meio de cédulas bancárias ou ordens de movimentação de conta-corrente via cheque.

A questão é distinta, contudo, quando os bancos – constatando que nem todos os depositantes

exigem o resgate dos depósitos em espécie – passam a operar com reservas fracionárias, violando os princípios gerais do direito, mantendo em custódia apenas uma fração do dinheiro físico que lhes foi depositado e emprestando o restante. Nesse arranjo, um banco pode simplesmente criar dinheiro do nada, ao expandir o crédito por um mero registro contábil, creditando "depósito à vista" do lado do passivo e debitando "empréstimo" do lado do ativo. Economicamente, os depósitos à vista desempenham a mesma função que um dinheiro material. Esse novo depósito à vista criado do nada é o que denominamos de moeda bancária ou escritural[86] [87].

Alcançamos agora o ponto exato a que precisávamos chegar. Descrevemos a evolução do dinheiro e do sistema bancário até o surgimento das reservas fracionárias e a criação do nada de depósitos à vista – note que ainda não introduzimos o surgimento dos bancos centrais e do sistema monetário atual de papel-moeda fiduciário; trataremos do atual arranjo mais adiante. Como dito acima, os depósitos à vista criados do nada, que desempenham perfeitamente a função de dinheiro e como tal são usados pelos indivíduos em suas transações, são também chamados de moeda bancária ou escritural. O problema com o primeiro termo, moeda bancária, é que ele ofusca a natureza dessa moeda, omitindo suas propriedades físico-químicas. Nas línguas latinas, esse mesmo termo é o mais comumente usado: *dinero bancário*, em espanhol; *monnaie bancaire*, em francês; e *moneta bancaria*, em italiano. No mundo anglo-saxão, *bank money* é o termo de preferência, enquanto no alemão usa-se *Bankgeld*. Nenhum desses termos transmite o real significado da moeda bancária.

Já no português, o termo moeda escritural é bastante difundido e é o que melhor representa a natureza dessa moeda. Como o próprio nome indica, moeda escritural é uma moeda que não existe materialmente senão nos livros de contabilidade do banco; existe apenas na forma *escrita*. E por que isso é importante para o nosso estudo do Bitcoin? Primeiro, porque isso demonstra que uma moeda intangível já existia[88] muito antes de uma moeda digital ser concebida pela mente humana, e, por fim, porque a existência de um bem intangível servindo como dinheiro jamais foi um empecilho para que indivíduos o usassem durante séculos.

Avançando até o presente, quando pensamos em dinheiro, normalmente o relacionamos a algo físico, material, como as cédulas em papel que carregamos na carteira ou as moedas metálicas de cobre. Mas também pensamos em todos os depósitos bancários de nossa propriedade, depósitos à vista e a prazo e poupança. Os dígitos de nossas contas bancárias são a moeda escritural moderna; a moeda escritural de hoje é, quase em sua totalidade, puramente digital. Um dos fatores que distinguem a ordem monetária e bancária moderna da de séculos passados é a presença de um banco central. O monopólio de emissão de moeda física (cédulas e moedas metálicas) é, normalmente, concedido pelos governos a esse órgão, o qual cria não somente moeda física, como também moeda escritural – na forma de reservas bancárias dos bancos. Da mesma forma, os bancos também têm a capacidade *de jure* e *de facto* de criar moeda escritural, mas a criação de moeda física lhes é vedada por lei. A capacidade de criação de moeda escritural pelos bancos, porém, não é ilimitada, sendo o banco central o ente responsável por controlar e coordenar – e até mesmo encorajar – a quantidade de moeda escritural passível de criação pelo sistema bancário.

Todavia, e ainda que esse arranjo seja verdadeiro, poder-se-ia indagar sobre a relevância da moeda escritural (intangível) atualmente. Pois bem, analisando os dados dos respectivos bancos centrais para mensurar a preponderância do dinheiro intangível no mundo moderno, constatamos que, na principal economia do planeta, a dos Estados Unidos, a moeda escritural representa mais de 55% do dinheiro em circulação. No Brasil essa relação é de 52%. Enquanto isso, nos países

da Zona do Euro, no Japão, na Suíça e na China, a moeda escritural responde por mais de 80% de toda a massa monetária. No Reino Unido, a moeda física não alcança nem 5% de todo o dinheiro em circulação[89].

Resta claro que a intangibilidade da moeda não é uma particularidade do Bitcoin. É, na verdade, uma característica marcante do sistema monetário desde o instante em que a moeda escritural foi criada do nada pela prática das reservas fracionárias. A intangibilidade da moeda é milenar. A escassez da moeda escritural, no entanto, sempre esteve sujeita ao controle de terceiros, bancos e bancos centrais. Com a criação do Bitcoin, essa vulnerabilidade foi sanada. E isso faz toda a diferença.

Do dinheiro commodity material (gado, sal, ouro ou prata), o mundo evoluiu ao papel-moeda e à moeda escritural. A intangibilidade desta permitiu aos bancos a criação quase ilimitada de moeda, corroendo continuamente o poder de compra do dinheiro que usamos. A intangibilidade do Bitcoin, por outro lado, propiciou justamente o oposto; assegurou a escassez da moeda, a fim de preservar – e não corroer – o seu poder de compra. Da intangibilidade do Bitcoin, também é possível evoluir – ou materializar – ao dinheiro físico. Alguns empresários, ávidos por satisfazer a demanda de alguns usuários, já criaram moedas físicas lastreadas em unidades monetárias de bitcoin[90]. Certamente, outras formas de moeda física com lastro em bitcoins surgirão no mercado.

4. Dinheiro, meio de troca ou o quê?

Poderíamos já considerar o Bitcoin um dinheiro? Em sua tese de mestrado[91], Peter Šurda afirma que não, Bitcoin ainda não é dinheiro. Tornar-se-á algum dia. Mas ainda não o é. Seguindo uma das definições da Escola Austríaca de Economia, “Bitcoin não é um meio de troca universalmente aceito”, afirma Šurda. Mas se não é dinheiro, então o que é? Seria um “meio de troca secundário” (conforme a definição de Mises em seu livro Ação Humana) ou uma quase-moeda (Rothbard, em seu livro *Man, Economy, and State*)?

Por outro lado, Graf levanta um ponto interessante: “Se dinheiro é definido como meio de troca universalmente aceito, então temos que qualificar o *universalmente*”[92]. Porque, se dissermos que dinheiro é o meio de troca “mais” universalmente aceito, “então certamente não chamaríamos Bitcoin de dinheiro”, conclui Graf, adicionando que “tampouco chamaríamos pesos mexicanos de dinheiro *dentro* dos Estados Unidos”. Entramos em uma área cinzenta, sem dúvida, mas há mérito no seu ponto. Graf concede que a única razão — ainda que passível de debate — para ainda não chamar Bitcoin de dinheiro reside no fato de que, “aparentemente, muitos usuários ainda enxergam os bitcoins através da lente da taxa de câmbio em relação às suas moedas locais”.

Em contrapartida, Frank Shostak afirma que Bitcoin “não é uma nova forma de dinheiro que substitui formas antigas, mas na verdade uma nova forma de empregar dinheiro existente em transações. Uma vez que Bitcoin não é dinheiro de verdade, mas meramente uma nova forma diferente de empregar a moeda fiduciária existente, ele não pode substituí-la”[93].

Contrariando Shostak, Bitcoin é um novo meio de troca, sim, ainda que não universalmente aceito. Ele é o que Mises classifica como dinheiro commodity ou dinheiro mercadoria. Mas não no sentido material, tangível, como normalmente se entende, e sim no sentido de “dinheiro

propriamente dito” (conforme o termo *money proper* usado por Mises em *Theory of Money and Credit*). O dinheiro propriamente dito é simplesmente o “bem econômico” usado como dinheiro, independentemente de qual bem este seja. Como esclarece Mises, “a característica decisiva de um dinheiro commodity é o emprego para fins monetários de uma commodity no sentido tecnológico… É uma questão de indiferença completa qual commodity em particular ela seja; o importante é que a commodity em questão constitua o dinheiro, e que o dinheiro é meramente essa commodity”[94].

A leitura da obra original em alemão, *Theorie des Geldes und Umlaufsmittel*, fornece mais pistas no sentido de entender que não importa qual mercadoria é usada como dinheiro; importa apenas que seja um bem econômico. Dinheiro commodity, em alemão, é “*Sachgeld*” (*sach*=coisa, *geld*=dinheiro), o que nos permite deduzir que qualquer “coisa” pode servir como dinheiro, contanto que seja usada e valorada como tal pelos indivíduos. Logo, uma unidade bitcoin, embora incorpórea, é o bem utilizado como meio de troca; o bitcoin é o próprio meio de troca, é o dinheiro propriamente dito[95] [96].

5. Ouro, papel-moeda ou bitcoin?

Recapitulando o caminho percorrido até aqui, descrevemos o nascimento da moeda digital e como ela em nada contraria a teoria da regressão de Ludwig Von Mises; abordamos a sua natureza intangível, bem como sua inerente escassez; e demonstramos como uma unidade bitcoin é o próprio meio de troca, ou o dinheiro propriamente dito. Vamos agora nos aprofundar um pouco mais na teoria e na prática, procurando comparar o sistema monetário atual – seja ele baseado em papel-moeda, seja baseado em ouro – com um sistema baseado em bitcoins. É preciso ressaltar, porém, que essa comparação se dá no campo conceitual e teórico, pois Bitcoin ainda não está no estágio avançado de vasta aceitação. Sua liquidez ainda é uma fração do sistema de papel-moeda fiduciária predominante no mundo todo.

Feitas as devidas ressalvas, poderíamos afirmar, então, que o Bitcoin é uma melhor alternativa ao sistema de moeda fiduciária atual ou até mesmo ao antigo padrão-ouro? Nikolay Gertchev constata que não, alegando que “não podemos ter um dinheiro que dependa de outra tecnologia (internet) e que, assim, o Bitcoin jamais atingiria o nível de universalidade e flexibilidade que o dinheiro material permite por natureza. Portanto, no livre mercado, dinheiro commodity, e presumivelmente ouro e prata, ainda têm uma vantagem comparativa”[97].

Somente podemos entender Bitcoin e contestar a crítica de Gertchev utilizando-nos da abordagem austríaca sobre a origem cataláctica do dinheiro. Em outras palavras, é entendendo que a origem do dinheiro se dá no mercado por meio de trocas voluntárias que podemos compreender a essência do fenômeno Bitcoin. Nesse sentido, faz-se necessário destacar que a introdução ou a evolução do dinheiro reduz os custos dos intercâmbios. Isto é, ao resolver o problema da dupla coincidência de desejos (tenho uma vaca, quero pão, e o padeiro quer um terno), a moeda vem a reduzir os custos envolvidos em uma simples troca de produtos. É o que os economistas chamam de “custos de transação”. Da mesma forma, em um entorno de concorrência, preponderará no mercado aquela moeda que mais reduz tais custos.

Em sua tese, Šurda elenca três elementos principais que influenciam na escolha de uma moeda: liquidez, reserva de valor e custos de transação. No momento, liquidez é a maior desvantagem do Bitcoin em relação às demais moedas, por não ser amplamente utilizado – ainda que cada vez

mais pessoas e empresas aceitam transacionar com a moeda.

No quesito reserva de valor, a sua escassez relativa, por sua vez derivada de sua oferta inelástica (atualmente em 12 milhões, com limite máximo de 21 milhões), permite-lhe ser considerada uma ótima alternativa na manutenção (e possivelmente elevação) do poder de compra. Ademais, por ser um meio de troca eletrônico, a moeda pode ser preservada indefinidamente – sim, dependemos da internet e da eletricidade.

É na redução dos custos de transação, porém, que entendemos as enormes vantagens e superioridade do Bitcoin. Para começar, não há fronteiras políticas à moeda digital. Você pode enviar e receber bitcoins de qualquer lugar a qualquer pessoa, esteja ela onde estiver, sem ter que ligar ao gerente do banco, assinar qualquer papel, comparecer a alguma agência bancária ou ATM. Nem mesmo precisa usar *VISA* ou *PayPal*. Você pode ter domicílio no Brasil, estar de férias em Xangai e enviar dinheiro a uma empresa na Islândia com a mesma facilidade com que envia um e-mail pelo seu iPhone. Ainda em Xangai, você pode receber em bitcoins o equivalente a quilos de prata (ou ouro, ou milhares de dólares), sem pesar um grama no seu bolso, nem mesmo precisar contar as suas cédulas ou pesar o seu metal. Tampouco precisa se preocupar em guardá-lo em algum armazém ou banco. Mais ainda, nem precisa se preocupar se seu banco guardaria de fato 100% do seu dinheiro ou acabaria usando-o para especulação em aventuras privadas.

Dessa forma, e de acordo com Šurda, é plenamente possível que, com o passar do tempo, o Bitcoin venha a superar tanto moedas fiduciárias quanto ouro e prata como meio de troca, e finalmente tornar-se dinheiro (meio de troca universalmente aceito). A questão-chave será a liquidez, que por sua vez depende da ampliação da aceitação da moeda. “Sem liquidez suficiente, Bitcoin enfrentará obstáculos significantes para evoluir a estágios mais maduros de meios de troca e, finalmente, dinheiro”, conclui Šurda.

Explicado tudo isso, resta claro que a crítica de Gertchev carece de fundamento. Considerando o atual arranjo monetário de moedas fiduciárias de papel, a maior parte da massa monetária é constituída de meros dígitos eletrônicos no ciberespaço, dígitos estes criados, controlados e monitorados pelo vasto sistema bancário sob a supervisão de um banco central. Dinheiro material ou físico é utilizado apenas em pequenas compras do dia a dia. O cerne do nosso sistema monetário *já* é digital e intangível.

Sei que Gertchev não julga esse arranjo como desejável, afinal de contas, não há lastro algum além dos PhDs que controlam a impressora de dinheiro. Mas mesmo em um sistema monetário lastreado 100% em um dinheiro material ou commodity, como o ouro, não escaparíamos do mundo virtual e eletrônico. Afinal de contas, carregar ouro (ou prata) por todo lugar não é nada eficiente, além de ser altamente perigoso em um país como o Brasil. Dessa forma, embora reconheça o mérito de um sistema monetário baseado no ouro – e efetivamente o considero como superior à alta discricionariedade atual –, jamais poderíamos prescindir do sistema bancário digital no presente estado da divisão internacional do trabalho. Um padrão-ouro sem um sistema bancário digital aliado ao uso de substitutos de dinheiro seria completamente inadequado à atual economia globalizada e interconectada.

Além disso, Gertchev parece não perceber que não é somente o atual sistema monetário que depende das tecnologias digitais e da internet, mas na verdade toda a economia globalizada e interconectada que conhecemos hoje. Bitcoin nasce nesse entorno, nasce da revolução digital e, certamente, não poderia sobreviver na ausência das tecnologias de que hoje dispomos. Tampouco poderia sobreviver a economia mundial, no estágio avançado em que se encontra, na ausência dessas mesmas tecnologias.

E não nos esqueçamos de que ouro ou papel-moeda também são formas de dinheiro que dependem de outras tecnologias. Ouro não cai do céu. Você precisa minerá-lo, cunhá-lo e transportá-lo. Quanta tecnologia e capital são necessários para desempenhar essas funções? E o que dizer dos altos custos com fretes e seguros envolvidos na movimentação de ouro de país para país, de continente a continente? Considero o metal precioso uma ótima alternativa à ordem monetária vigente, sem dúvida alguma. Mas julgo que a sua grande qualidade como meio de troca jaz na sua escassez relativa, na sua oferta inelástica. Ouro é excelente como reserva de valor, mas sem um sistema eletrônico de pagamentos, o metal seria muito pouco eficiente no quesito "transportabilidade". A grande revolução do Bitcoin é capacidade de replicar a inerente escassez relativa do ouro, mas sem incorporar a grande desvantagem do metal no que tange ao manuseio e transporte, especialmente em longas distâncias.

Outra vantagem sem precedentes reside em uma tecnicalidade, à primeira vista trivial, mas de implicações extraordinárias. Primeiro, você não depende do sistema bancário no mundo dos bitcoins. Você é seu próprio banco. E isso não é tudo. Devido às regras e à criptografia empregada, é impossível duas pessoas gastarem a mesma moeda digital (gasto duplo). Isso quer dizer que somente uma pessoa detém o direito de propriedade de uma unidade monetária e somente essa pessoa a controla. E isso ainda não é tudo. No mundo atual de papel-moeda fiduciária, os dígitos da sua conta bancária são substitutos de dinheiro físico (cédulas e moedas metálicas). O dinheiro propriamente dito é o papel-moeda. Ou melhor, uma fração dos seus depósitos é dinheiro físico.

No caso do Bitcoin, a unidade monetária (1 BTC) é o próprio equivalente ao dinheiro físico atual, ele é o próprio bem monetário. E é nesse ponto que surge algo de consequências singulares. Substitutos de dinheiro emergem somente quando oferecem uma redução nos custos de transação. Isso quer dizer que os substitutos de dinheiro serão demandados quando proporcionarem ao usuário algo que o dinheiro próprio (dinheiro commodity) não é capaz de oferecer. Pela sua natureza e propriedades digitais, os bitcoins já propiciam muitos dos serviços normalmente restritos aos substitutos de dinheiro. Seus custos de transação são suficientemente reduzidos, tornando altamente improvável o surgimento desses substitutos. Logo, e de uma só vez, o Bitcoin não só tem o potencial de tornar o sistema bancário em grande parte irrelevante e obsoleto, como também reduz substancialmente a probabilidade do aparecimento das reservas fracionárias[98] e, portanto, a expansão artificial de crédito, evitando assim a formação de ciclos econômicos.

A grande sacada do Bitcoin, talvez uma de suas maiores vantagens, é que a moeda digital dispensa o intermediário, o "terceiro" na transação. É um sistema *peer-to-peer*. Não é necessário confiar em um banco que guardará seu dinheiro. Você tampouco precisa assegurar-se de que uma empresa de liquidação de pagamentos processará corretamente o seu pedido. Acima de tudo, você não precisa rezar para que um banco central não deprecie a moeda. "Um ponto comum nos atributos avançados do Bitcoin é a reduzida necessidade de confiança no fator humano," observa Šurda; "a confiança é substituída por comprovação matemática". É a criptografia moderna garantindo a solidez da moeda.

Ademais, o caráter dual do método de pagamentos pode ser visto como a combinação das características do dinheiro (commodity) com o sistema de liquidação (serviço). "Enquanto a commodity oferece uma oferta estável e controle físico, o serviço permite baixos custos de transação, serviços de liquidação e registros históricos", conclui Šurda; "antes do Bitcoin, essas duas funções estavam separadas". Logicamente, ainda não estamos nesse estágio avançado do Bitcoin, porque sua liquidez ainda é baixa e ainda dependemos bastante das "casas de câmbio" –

os pontos de contato entre a rede Bitcoin e o mundo de moedas fiduciárias. Mas o sistema permite que esse ideal seja alcançado.

Por todos esses motivos, pode-se dizer que o Bitcoin é o arranjo monetário que mais se aproxima daquele idealizado pelos economistas da Escola Austríaca. Como muito bem destaca Šurda, "É, historicamente, a primeira oportunidade de se atingir a mudança e a manutenção de uma oferta monetária inelástica sem reformas legais e sem precisar endereçar as reservas fracionárias".

Por fim, comparemos os diversos atributos monetários do ouro, do papel-moeda e do Bitcoin. No quesito durabilidade, Bitcoin supera tanto o ouro quanto o papel-moeda – salvo no improvável caso de a internet inexistir no globo terrestre. Bens digitais como um bitcoin não sofrem alteração espacial ou temporal. No entanto, uma barra de ouro está sujeita ao desgaste natural do uso, perdendo massa ao longo do tempo. Já o papel-moeda é bastante frágil, podendo ser destruído facilmente. Embora seja verdade que, enquanto na forma de substitutos de dinheiro em contas-correntes eletrônicas, o papel-moeda é tão durável quanto o Bitcoin.

No que tange à divisibilidade, há um limite físico pelo qual o ouro pode ser fracionado, o que não ocorre com o papel-moeda – qualquer denominação pode ser impressa em uma cédula. O Bitcoin, porém, é perfeitamente divisível, com oito casas decimais e possibilidade de adicionar quantas mais forem necessárias.

Ambas as formas de moeda tangível, ouro e papel-moeda, são bastante maleáveis, o que é irrelevante ao Bitcoin, por ser um bem essencialmente incorpóreo.

O Bitcoin é, então, durável e perfeitamente divisível, embora incorpóreo. Ademais, um bitcoin é insuperavelmente uniforme, porque sua homogeneidade é matemática (por definição) e não física (não depende de medições empíricas relativas a um padrão)[99], sendo tecnicamente impossível falsificá-lo. O ouro, ao contrário, depende de verificações e comprovações quanto a sua pureza e massa. Já o papel-moeda, embora seja bastante homogêneo, pode ser mais facilmente falsificado, dificultando a distinção de unidades monetárias genuínas das ilegítimas.

É na sua escassez relativa, contudo – intrínseca, autêntica e intangível –, que o Bitcoin se sobressai quando contrastado com o metal precioso e com as moedas de papel. Assegurada por meio da criptografia e da ausência de terceiros fiduciários capazes de aumentar a oferta monetária por meio da emissão de substitutos de moeda, a oferta inelástica de bitcoins é parte inseparável do seu protocolo. Ainda que o ouro também seja naturalmente escasso, seu emprego monetário depende em larga medida de um sistema bancário e de liquidação, tornando provável o aparecimento de substitutos de dinheiro não lastreados no metal, enfraquecendo a sua natural escassez. Não obstante, a oferta inelástica do ouro – ora contornada pela emissão de substitutos monetários – é muito superior à ilimitada capacidade de impressão de papel-moeda pelos bancos centrais, capacidade essa potencializada pela introdução dos meios eletrônicos na criação de moeda escritural, seja pelos bancos, seja pela autoridade monetária, e operacionalizada de forma discricionária e, frequentemente, por decisão política.

E, finalmente, o Bitcoin reúne em um mesmo sistema serviços comumente providos por uma quantidade enorme de intermediários, como bancos, casas de liquidação, bancos centrais, entidades interbancárias internacionais, etc., enquanto um sistema monetário baseado no ouro ou em papel-moeda jamais poderia dispensar tais terceiros fiduciários.

Na tabela abaixo, podemos visualizar de forma resumida os atributos de cada um dos sistemas monetários analisados:

Atributos	Ouro	Papel-moeda	Bitcoin
1. Durabilidade	Alta	Baixa	Perfeita
2. Divisibilidade	Média	Alta	Perfeita
3. Maleabilidade	Alta	Alta	Incorpóreo
4. Homogeneidade	Média	Alta	Perfeita
5. Oferta (Escassez)	Limitada pela natureza	Ilimitada e controlada politicamente	Limitada matematica-mente
6. Dependência de terceiros fiduciários	Alta	Alta	Baixa ou quase nula

O Bitcoin é, simplesmente, uma forma de moeda superior a todas as demais. Incorpora a escassez relativa do ouro, aliada à instantânea transportabilidade e divisibilidade dos substitutos de dinheiro (especialmente aqueles na forma digital moderna), prescindindo de inúmeros terceiros fiduciários – como bancos, casas de liquidação e entidades interbancárias internacionais –, eliminando, assim, o risco da contraparte.

6. Deflação e aumento do poder de compra, adicionando alguns zeros

Para diversos economistas, uma grande desvantagem da moeda digital é a *deflação que o Bitcoin geraria*. Em primeiro lugar, é preciso definir os termos. Na acepção correta da palavra, deflação significa uma contração da base monetária. Ora, isso é tecnicamente impossível. A quantidade máxima de bitcoins que podem ser minerados é de 21 milhões. Mineradas todas as unidades monetárias, não há possibilidade de a base monetária diminuir ou contrair-se. O que pode acontecer é usuários perderem suas senhas e jamais poderem usar suas carteiras novamente, o que os impossibilita de acessar suas contas e transacionar. Mesmo nesse caso, os bitcoins não seriam destruídos, apenas não mais seriam utilizados. A consequência, por ficarem "fora" de circulação, seria um aumento no poder de compra do restante de bitcoins existentes.

Entretanto, costuma-se associar o termo deflação a uma queda dos preços. Infelizmente, redução de preços supõe um problema para a maioria dos economistas. À população, isso significa que seu poder de compra aumentou. Uma moeda que se aprecia ao longo do tempo com certeza não representa nenhuma ameaça à saúde de uma economia[100].

Não é o foco deste livro discorrer sobre os problemas e consequências da inflação ou deflação. Há diversas obras dedicadas ao assunto. Entretanto, por ser algo que tange à essência do Bitcoin, não podemos nos esquivar de aprofundar um pouco mais esse tema. Em termos de teoria econômica, o problema jaz em compreender se um aumento ou diminuição da quantidade de dinheiro são capazes de gerar benefícios ou malefícios à economia. Uma economia em desenvolvimento precisa de uma oferta monetária crescente? Ou o ajuste pode se dar via preço da moeda – o que significa que ela ganha poder aquisitivo? Aumentar a quantidade de dinheiro na economia, inflação, não gera nenhuma prosperidade. Não cria novos bens e serviços do nada. Apenas os torna mais caros. A inflação monetária tem um efeito redistributivo de riqueza. Aqueles que primeiro recebem o dinheiro recém-criado podem gastá-lo adquirindo produtos a preços atuais. À medida que a moeda circula pela economia, aumentando os preços dos bens e serviços, os últimos a recebê-la perceberão que seus salários não podem mais comprar a mesma

quantidade de produtos que antes era possível.

Inflacionar a oferta monetária, portanto, não é uma política neutra. Existem ganhadores e perdedores. E para que uma economia cresça, não há uma quantidade de dinheiro ideal. Qualquer quantidade basta[101]. Os problemas surgem quando a oferta de moeda sofre aumentos e diminuições repentinos e intensos devido às decisões políticas.

No caso do Bitcoin, a oferta crescerá de forma paulatina, pré-estabelecida e conhecida por todos os usuários até alcançar o limite máximo de 21 milhões de unidades ao redor do ano de 2140. Mas cerca de 90% de todos os bitcoins já estarão minerados por volta de 2022. Assumindo que a demanda por bitcoins continue crescendo ao longo dos próximos anos, isso significaria que uma unidade bitcoin valeria cada vez mais. E quanto mais se amplie a aceitação da moeda, maior será seu poder de compra. Em face dessa constatação, os economistas leigos em Bitcoin alegam que será quase impossível usar uma unidade de bitcoin em compras do dia a dia, pois ela valerá muito no futuro. O que lhes escapa é o fato de que os bitcoins são perfeitamente divisíveis. Cada bitcoin conta com oito casas decimais. Isso permite aos usuários realizar transações com frações de um bitcoin[102]. E se chegarmos ao estágio avançado de algum dia 0,00000001 BTC (ou 1 “satoshi”, como é denominada a oitava fração de um BTC) valer tanto que seja preciso mais casas decimais? Felizmente, é possível aumentar a quantidade de casas decimais por meio do consenso entre todos os usuários da rede Bitcoin. O sistema está preparado para tal aperfeiçoamento.

Ao cidadão brasileiro, escaldado por um passado não tão distante de altas e hiperinflações, essa peculiaridade do Bitcoin equivale ao inverso do que ocorreu algumas vezes no Brasil das décadas inflacionárias: o corte de zeros. Porque o governo inflacionava tanto a moeda nacional, o Banco Central chegou ao extremo de imprimir cédulas de Cr$ 500.000 (quinhentos mil cruzeiros, em 1993). Dessa forma, tornava-se progressivamente mais difícil transacionar em denominações tão altas. Muitos brasileiros ficaram milionários, embora extremamente pobres. Pouco podiam comprar com a moeda, que perdia valor a cada hora. E a cada nova reforma monetária, vinha uma nova moeda e o corte de três zeros. De 1942 até 1993, houve cinco instâncias em que o corte de três zeros foi adotado, sendo que três delas nos últimos sete anos desse período[103]. A lógica dos cortes de zeros era retornar às denominações menores, para simplificar as contas do dia, bem como dar a impressão de que alguma reforma efetiva havia sido levada a cabo, quando, em realidade, as causas da inflação monetária permaneciam em pleno funcionamento.

E qual a equivalência inversa desse período brasileiro com o Bitcoin? Da mesma forma que transacionar com denominações cada vez maiores se torna um complicador adicional às atividades do cotidiano (milhão ou bilhão eram cifras de uso comum), denominações cada vez menores de bitcoin tornarão o uso da moeda um tanto complicado. Qual a solução? Adicionar três zeros à unidade monetária. Dessa forma, 1 BTC passaria a ser 1.000 BTC. Em uma hiperinflação, cortam-se zeros. Em uma hiperdeflação, adicionam-se zeros[104] – este evidencia a constante apreciação de valor; aquele, a constante perda de valor. Pelo consenso entre os usuários da rede, uma mudança como essa poderia ser efetuada no protocolo do Bitcoin. Inclusive, porque a cotação de um bitcoin já chegou a mais de 1.000 dólares, discussões nesse sentido já foram iniciadas na comunidade.

7. O preço do bitcoin, oferta e demanda

No dia 5 de outubro de 2009, *nove meses depois* de a rede Bitcoin ter começado a operar, o primeiro registro de preço de venda de um bitcoin ofertado foi publicado. Um total de 13 bitcoins por centavo de dólar, ou especificamente 1.309,03 bitcoins por um dólar, calculado pelo ofertante com base em seus custos variáveis de mineração.

Alguns meses depois, em maio de 2010, uma pizza foi vendida por 10 mil BTC, equivalente a 25 dólares à época. Mas, em realidade, essa não foi uma transação genuína, pois o comprador transferiu 10 mil BTC a um terceiro, que facilitou a compra por cartão de crédito na pizzaria. Ainda assim, a compra foi um registro do preço de um bitcoin então, 4 BTC por centavo de dólar. Somente em 17 de julho de 2010 ocorreu o primeiro registro de uma transação em uma casa de câmbio, a Mt.Gox, em que um bitcoin era negociado a US$ 0,05. A partir desse momento, novas transações iam sendo efetuadas, e o processo de descobrimento do preço de um bitcoin ganhou cada vez mais tração e volume[105].

Durante o ano 2013, o preço de um bitcoin ultrapassou 1.000 dólares, sendo atualmente negociado levemente abaixo desse patamar[106]. Mas estaria o preço de um bitcoin caro ou barato? Não saberíamos dizer. E a verdade é que ninguém sabe. O ponto fundamental não é se 1 BTC vale 1.000 ou 30 dólares, mas sim que o preço de uma unidade bitcoin está acima de zero, e isso, por si só, já é surpreendente. O simples fato de a moeda digital ter um preço e estar sendo utilizada por indivíduos em intercâmbios já é um feito em si.

Estamos ainda na infância do experimento Bitcoin. A cotação de um bitcoin em relação a outras moedas, ou o seu *preço*, é algo que está sendo descoberto pelo mercado, e não podemos prever a sua evolução. E ainda que, pelo lado da demanda, não saibamos como ela evoluirá, ao menos do lado da oferta não seremos surpreendidos por súbitos aumentos na quantidade de bitcoins em circulação.

É claro que a alta volatilidade testemunhada em alguns períodos específicos ao longo dos últimos dois anos complica a vida dos usuários de bitcoins — e talvez facilite a dos especuladores —, e é por esse fator que, quanto maior o número de aderentes, mais benéfico será para o avanço da moeda digital. Mas não interpretemos esse argumento como um convite à especulação. Quanto mais indivíduos aderirem e utilizarem a moeda, maior será sua liquidez. Quanto mais liquidez, menor tende a ser a sua volatilidade e aceitação no mercado. No entanto, uma maior liquidez não necessariamente significa um *preço* maior.

Alguns afirmam tratar-se apenas de uma nova bolha que em breve estourará levando seus usuários à ruína. Será que estamos presenciando uma bolha de fato? Pode ser que o Bitcoin, sim, esteja em uma *fase* de bolha. Pode ser que não. Não sabemos. Mas uma bolha especulativa em si não é um fator preponderante para o avanço e futuro do Bitcoin. A bolha da internet no início dos anos 2000 não decretou o fim da internet, e a mania das tulipas, séculos atrás, tampouco fez a lilácea desaparecer do mercado.

De certa forma, o preço de uma unidade BTC é irrelevante. A questão-chave é que a moeda digital tem verdadeiras vantagens comparativas, oferecendo excelentes serviços de pagamentos e reduzindo de forma significativa os custos de transação. Como diz Tony Gallipi, sócio do site de pagamentos BitPay, “Bitcoin é simplesmente a maneira mais fácil até hoje inventada de enviar dinheiro de A para B”.

8. Valor intrínseco ou propriedades intrínsecas?

A mais frequente objeção, no entanto, é outra. E, segundo aqueles que a ela recorrem, é a questão básica e fundamental: Bitcoin não tem valor intrínseco, ele não é uma "coisa". É uma unidade de uma moeda virtual não material. Não tem nenhuma condição ou formato físico, e, portanto, é descabida a noção de que possa algum dia substituir a moeda fiduciária. Esse é o núcleo do argumento de tais céticos.

O que lhes parece escapar, contudo, é que não existe *valor* intrínseco, existem *propriedades* intrínsecas (químicas e físicas). Valor é subjetivo e está na mente de cada indivíduo. "Bitcoin é o ouro digital"[107], defende Jon Matonis, conselheiro da Fundação Bitcoin, "mas em vez de depender de propriedades químicas, ele depende de propriedades matemáticas". Isso quer dizer que as propriedades do Bitcoin resultam do design do sistema, permitindo que sejam valoradas subjetivamente pelos usuários. Essa valoração é demonstrada quando indivíduos transacionam livremente com bitcoins.

Admitindo a fragilidade de seu argumento, os céticos partem para outra crítica, a de que o Bitcoin, além do seu valor de troca (ou seu valor monetário), não apresenta nenhum *valor de uso* amplamente reconhecido, ou *uso não-monetário*. Por esse motivo, raciocinam eles, a moeda digital não poderia jamais adquirir o *status* de meio de troca universalmente aceito no comércio. Isso me faz perguntar: como o ouro conseguiu emergir como dinheiro, sendo que seu principal valor de uso séculos atrás era basicamente adorno e enfeite? Sim, é claro que hoje em dia o ouro tem aplicação nos mais diversos campos (indústria, medicina, computação, etc.), mas essa demanda surgiu com relevância somente nos últimos 20 ou 30 anos. E mesmo considerando seu uso industrial, estima-se que mais de 90% da demanda por ouro derivem de seu uso monetário.

Em suma, e conforme já detalhado anteriormente, não proporcionar uma maior variedade de aplicações e uso, ou, dito de outra forma, não ter um *uso não-monetário* amplamente reconhecido não impede que o Bitcoin venha a ser um meio de troca universalmente aceito. Ao menos *a priori*, tal assertiva não pode ser considerada conclusiva.

9. A falta de lastro aparente não é um problema

Semelhante à crítica de carência de valor intrínseco, a constatação de que o bitcoin é desprovido de lastro leva inúmeros economistas a taxar a moeda digital de débil e inerentemente defeituosa. A realidade é que o Bitcoin tornou evidente algo até hoje pouco compreendido: lastro não é uma necessidade teórica de uma moeda, apenas uma tecnicalidade empírica cujo principal serviço foi o de servir como restrição às práticas imprudentes de banqueiros e às investidas inflacionistas do estado no gerenciamento da moeda.

Historicamente o dinheiro escolhido pelo mercado por excelência, o ouro foi o principal ativo utilizado como lastro pelos bancos ao longo da história. Em primeiro lugar, porque os certificados de depósito, bilhetes de banco ou depósitos à vista eram meras representações da moeda propriamente dita, o ouro. Eram substitutos monetários aceitos como se a moeda fossem, devido à qualidade explícita de poderem ser convertidos em espécie quando solicitado ao banco pelo portador. Segundo, a obrigatoriedade de lastrear qualquer emissão de bilhetes ou certificados de depósito com o ouro impunha certa disciplina à prática bancária. Aqueles bancos que emitissem mais bilhetes do que ouro em custódia estariam mais facilmente sujeitos à insolvência no instante em que os clientes questionassem a presença de lastro em posse do banco e exigissem em massa o resgate em espécie.

Entretanto, com a consagração do sistema de bancos centrais nos últimos dois séculos, o lastro em ouro tomou contornos um pouco distintos. Embora fosse o ouro a moeda global durante milênios, as diferentes nações emitiam suas próprias moedas de papel dentro de suas jurisdições, vale notar, sempre lastreadas no metal precioso. Historicamente, as moedas nacionais nada mais eram do que denominações de certa massa de ouro ou prata. A “libra esterlina” inglesa, por exemplo, era a denominação originalmente dada a uma libra de prata. Quando os governos se arrogaram o monopólio de emissão da moeda, a política monetária na prática restringia-se, em certa medida, a manter a paridade entre o valor de face do bilhete de banco (emitido monopolisticamente pelo estado) e seu valor de mercado. À medida que os governos inflacionavam a oferta de bilhetes, o valor de mercado deste se depreciava, incitando os portadores a resgatar em espécie pelo valor de face, ou “resgatar ao par”. Tinham início, assim, os dilemas dos monopolistas da emissão de moedas nacionais: retirar de circulação o excesso de bilhetes, buscando manter seu valor de face? Assumir a inépcia na condução das questões monetárias, desvalorizando oficialmente o valor de face dos bilhetes emitidos? Ou, o pior dos casos, suspender temporariamente a conversibilidade em espécie, em moeda propriamente dita (ouro ou prata)?

Especialmente a partir do fim do século XIX, o ouro pouco circulava na economia. Os intercâmbios no mercado davam-se, na sua maior parte, por meio dos papéis-moedas nacionais ou dos depósitos à vista com o uso de cheques. Logo, a função monetária desempenhada pelos metais preciosos nos últimos séculos foi, primordialmente, a de servir como uma âncora de valor, como um disciplinador às tentativas de inflacionar os papéis-moedas nacionais. Sob o ponto de vista do governo, portanto, nada mais lógico do que buscar remover qualquer vínculo ou lastro ao metal precioso para poder emitir moeda sem qualquer tipo de restrição[108]. Dessa forma, o ouro serviu como lastro para que tivéssemos a segurança (ou esperança) de que a oferta monetária não seria inflada pela emissão excessiva de substitutos de dinheiro, sejam cédulas, sejam depósitos à vista.

Mas façamos um experimento mental. Imaginemos que, em um sistema em que os substitutos de dinheiro (cédulas e depósitos à vista) são os meios circulantes principais e supostamente lastreados 100% em dinheiro propriamente dito (ouro, por exemplo), descobríssemos um método de garantir efetivamente que haveria, a todo instante, 100% de reservas em dinheiro para os substitutos emitidos, tornando, assim, desnecessária a prática de resgatar em espécie como forma de impor disciplina aos bancos. Nesse caso, surge a pergunta: se o ouro em custódia nos cofres dos bancos serve unicamente para restringir a expansão de meios fiduciários (substitutos de moeda sem lastro), serviria ele para alguma função no momento em que descobrirmos essa maneira perfeitamente segura de impedir expansão irrestrita de meios fiduciários?

No atual sistema de inconversibilidade absoluta dos papéis-moedas nacionais – não há qualquer lastro em ouro, o papel-moeda tornou-se a moeda propriamente dita –, a experiência de mais de quase meio século comprovou que banco central nenhum conseguiu abster-se do poder de emissão de dinheiro, depreciando as respectivas moedas nacionais em uma espécie de corrida ao fundo do poço ao longo de todos esses anos. Com o Bitcoin, o dilema da provisão da oferta monetária foi equacionado: a emissão será realizada de forma competitiva e paulatinamente, a uma taxa de crescimento preestabelecida, limitada a 21 milhões de unidades. Uma legítima escassez, intangível, e matemática e criptograficamente assegurada.

Qual o lastro do ouro? A escassez inerente a suas propriedades físico-químicas. Qual o lastro do papel-moeda fiduciário? A confiança de que governos não inflacionarão a moeda, apoiada em leis de curso forçado que obrigam os cidadãos a aceitar a moeda como pagamento. Qual o lastro

do Bitcoin? Propriedades matemáticas que garantem uma oferta monetária, cujo aumento ocorre a um ritmo decrescente a um limite máximo e pré-sabido por todos os usuários da moeda. Após um bem ser empregado e reconhecido como moeda, seu lastro jaz na sua escassez relativa.

Mas qual a distinção-chave entre o lastro do ouro e o do Bitcoin e o lastro das moedas estatais? O lastro físico é naturalmente provido de ou pretende assegurar uma escassez de oferta, assim como o lastro matemático do Bitcoin. O lastro governamental, porém, garante unicamente uma demanda mínima, mas não uma oferta inelástica. Em outras palavras, o lastro estatal não assegura uma moeda boa, apenas que até uma moeda ruim tenha vasta aceitação no mercado.

10. A política monetária do Bitcoin

É importante entendermos a política monetária do Bitcoin, especialmente em comparação às das autoridades monetárias vigentes em cada estado-nação. Mas antes de detalharmos a operação da política monetária da moeda digital, é útil compreendermos como tal política funciona na era dos bancos centrais.

As autoridades monetárias ao redor do mundo, desde o primeiro banco central do planeta – o Riksbank, da Suécia, em 1668 – até o presente, introduziram, testaram e aprimoraram diversas ferramentas e estratégias distintas na condução de suas responsabilidades e funções. A política monetária atual, na forma como é realizada, pouco se assemelha àquela dos primórdios dos bancos centrais. O resultado prático de todas as ferramentas empregadas para efeito de política monetária, no entanto, é basicamente o de manipular a oferta de moeda na economia.

O aprimoramento da prática moderna do banco central deu-se especialmente durante a segunda metade do século XX. Após o fim da conversibilidade do dólar em ouro – o que também significou o fim da conversibilidade de qualquer moeda nacional em ouro –, os bancos centrais estavam livres das restrições impostas pelo lastro no metal precioso. Isso teve implicações importantes. Desprovida da âncora do ouro, a autoridade monetária perde uma forte referência de controle da oferta de moeda – quando se emite moeda nacional em excesso, o ouro tende a fluir para fora do país, forçando o banco central a adotar uma política contracionista da oferta monetária. Por outro lado, a ausência da âncora significou que os bancos centrais estavam agora livres para inflar a oferta de papel-moeda ilimitadamente. Mas qual aumento seria razoável? Que efeitos teria em uma economia um incremento de 5% anual na quantidade de moeda em circulação? Quais partes da oferta monetária deveriam ser alvo da política do banco central: papel-moeda, reservas bancárias, depósitos à vista? Como controlar a criação de moeda pelo sistema bancário? Para o bem ou para o mal, o fim do padrão-ouro deu início à era da liberdade e discricionariedade dos banqueiros centrais.

Diante de tantos dilemas, a era moderna dos bancos centrais é notória por estar assentada em um processo explícito[109] de tentativa e erro. Em geral, a política monetária logo após o fim de Bretton Woods tinha como meta um crescimento específico da oferta monetária. Obviamente, o percentual definido e os agregados monetários sujeitos à meta eram decididos arbitrariamente. Nesse arranjo, a taxa de juros era consequência e não alvo da política monetária. Entretanto, a turbulenta década de 70 e as crises financeiras da de 80 obrigaram as autoridades monetárias a rever seu ferramental. O fim do século marcou, então, o período da política monetária de taxa de juros, em que a variável era alvo direto das ações do banco central, estabelecendo-a como meta, sendo o crescimento da oferta monetária mero produto da política de juros.

O dilema atual é como calibrar a taxa de juros de modo a fomentar uma atividade econômica estável e sustentável. Para levar a cabo tal empreitada, o ferramental acessório é vasto, e vai desde o nível do compulsório e operações de mercado aberto até as diversas regulações emitidas pela autoridade monetária de cada país. Resumidamente, e o que nos interessa neste contexto, a política monetária objetiva manipular a oferta de moeda em uma economia. No passado, deu-se de forma direta, com alvos específicos para o crescimento de algum agregado monetário. Atualmente, a manipulação da oferta monetária ocorre indiretamente, pela influência direta sobre a taxa de juros.

A política monetária do Bitcoin, por sua vez, foi estabelecida na sua criação e pode ser definida como uma política monetária baseada em regras[110], cuja independência é assegurada pela natureza distribuída da rede subjacente. Essa política monetária não discricionária pode ser mais bem descrita como "meta de oferta monetária assintótica"[111] (MOMA). A unidade monetária chama-se bitcoin, e sua emissão ocorre por meio de subcontratados chamados de mineradores, os quais desempenham os cálculos de Prova de Esforço (PoE, ou *Proof-of-Work*, *PoW*), que garantem a independência da política monetária e processam os pagamentos. "A senhoriagem subsidia o sistema de pagamento ao invés de beneficiar exclusivamente o emissor ou o vendedor/receptor de títulos negociados em operações de mercado aberto. A senhoriagem da PoE e a MOMA trabalham de forma sinérgica causando três fenômenos monetários" [112]: i) agentes econômicos racionais mantêm encaixe em bitcoins mesmo não tendo nenhum passivo denominado em bitcoins; ii) o mercado estabelece as taxas de câmbio e de juros, sem exceção; e iii) é altamente improvável o aparecimento das reservas fracionárias.[113]

Os agentes econômicos decidem livremente manter saldos em bitcoins devido a todas as vantagens da moeda digital perante outras formas de dinheiro e à expectativa de que essas vantagens conduzirão outros agentes a adotar bitcoins no futuro, possivelmente apreciando sua taxa de câmbio.

Sob a perspectiva da Trindade Impossível[114], foi estabelecido para o Bitcoin uma política monetária independente e liberdade total nos fluxos de capitais. Nenhuma entidade intervém em ciclos de alta e apreciação especulativa de modo a estabilizar a taxa de câmbio. A independência é assegurada, propiciando aos agentes econômicos uma perfeita previsibilidade da oferta monetária futura. Como explicado previamente, o limite máximo de 21 milhões é desimportante, uma vez que há perfeita divisibilidade das unidades monetárias de bitcoins. Qualquer ajuste necessário será refletido pelo mercado na taxa de câmbio. E, finalmente, assim como o ouro, o bitcoin não é passivo de nenhuma instituição; é um ativo sem risco de contraparte.

11. As reservas fracionárias, o *tantundem* e o Bitcoin

Sob a perspectiva econômica, a probabilidade de aparecimento das reservas fracionárias no sistema Bitcoin é bastante reduzida. Porque o Bitcoin oferece aos usuários as vantagens tecnológicas tanto do dinheiro commodity propriamente dito quanto de um substituto de dinheiro (como certificados de depósitos, os precursores do papel-moeda), o aparecimento de um substituto de uma unidade monetária de bitcoin seria, até certo ponto, redundante.

Historicamente, o substituto de dinheiro surgiu como uma forma de reduzir os custos de transação, permitindo um uso mais eficiente do dinheiro, usos que com o dinheiro commodity em si não seriam possíveis. O sistema Bitcoin sobressai-se justamente nesse ponto, pois a base

monetária bitcoin em si já propicia uma redução substancial dos custos de transação quando comparada aos sistemas monetários atuais. Como explicado anteriormente, o Bitcoin é ao mesmo tempo uma moeda e um sistema de pagamentos, algo sem precedentes na história monetária. Mas seria possível conceber a prática de reservas fracionárias com bitcoins? Sim, é possível. Para entendermos como, é preciso ir ao básico ou à origem da atividade bancária: o depósito de dinheiro.

Os bancos surgiram para suprir uma necessidade de mercado, o serviço de custódia de bens monetários. Com o aperfeiçoamento da prática bancária, eles passaram a oferecer não somente o serviço de custódia, mas também de intermediação financeira e de facilidade de pagamentos. É no desenvolvimento do serviço de custódia, contudo, que graves consequências se sucedem. A custódia de dinheiro requer um contrato de depósito entre banco e depositante em que este deposita *bens fungíveis* para que o banco os guarde, os custodie e os restitua a qualquer momento quando solicitado pelo depositante[115]. Em troca, ao depositante é entregue um certificado de depósito que lhe dá o direito de exigir a restituição do depósito a qualquer momento. Entretanto, ao tratar-se de bens fungíveis, não é obrigatório que o banco restitua o cliente com as *mesmas moedas ou barras de metal* precioso que lhe foram depositadas; basta entregar ao depositante uma quantidade equivalente em gênero e qualidade, ou *tantundem*, em latim.

Com o desenvolvimento da prática bancária, os certificados de depósitos evoluíram a bilhetes de banco – bastava o portador apresentar o bilhete no caixa para ter restituído seu dinheiro em espécie –, os quais passaram a circular como se o próprio dinheiro fosse. Os bancos logo perceberam que os depositantes raramente resgatavam seus depósitos, preferindo, em vez disso, transacionar somente com os bilhetes (substitutos de dinheiro), pela praticidade e facilidade de manuseio. Diante dessa constatação, não tardou muito para que as instituições bancárias cometessem um grave delito, o de emitir bilhetes sem lastro algum em dinheiro material. Iniciava assim a prática das reservas fracionárias, em que havia mais bilhetes em circulação emitidos pelos bancos do que dinheiro material em custódia para a pronta restituição de quem assim demandasse[116]. Dessa forma, quando a confiança em alguma instituição depositária fosse abalada e os depositantes se dirigissem em massa para solicitar o resgate em espécie de seus bilhetes – a notória corrida bancária –, o banco estaria simplesmente insolvente; não poderia jamais entregar dinheiro material a todos os demandantes portadores de bilhetes. Não haveria *tantundem* suficiente em custódia.

Os registros da prática de reservas fracionárias ao longo da história são milenares, mas seu ápice foi atingido somente no século passado, com a anuência e auxílio dos bancos centrais. Hoje em dia, a prática não somente é regra do sistema bancário em escala global, como também é respaldada por lei[117].

E como o Bitcoin difere desse arranjo? Em primeiro lugar, quando temos o cliente Bitcoin instalado e rodando em nosso computador pessoal, não há um contrato de depósito entre proprietário de bitcoins e um banco ou casa de custódia. Você é seu próprio banco. Você custodia o seu próprio *tantundem*. Logo, a posse dos bitcoins está a todo o instante com o dono da carteira (equivalente à conta bancária tradicional). Igualmente, ao proprietário, há disponibilidade completa e irrestrita dos bitcoins. Você pode transferi-los a quem desejar a todo instante sem que nenhuma entidade o impeça de fazê-lo.

Mas é claro que, se dependermos exclusivamente do software em um computador pessoal, o uso do Bitcoin seria bastante reduzido. Para suprir essa necessidade, já foram criados serviços de

carteira online, como o da empresa *blockchain.info*, em que podemos usar um smartphone ou equipamento portátil similar para efetuar transações. Ainda que à primeira vista tenhamos a impressão de que isso constitui um serviço de custódia similar ao oferecido pelo sistema bancário tradicional, há uma grande distinção. Nos serviços de carteira online como o exemplificado acima, o provedor não custodia os seus bitcoins. Na verdade, você permanece sendo o único agente a ter posse, controle e uso irrestrito dos seus bitcoins. Da forma como é configurado esse serviço, o provedor proporciona ao usuário a capacidade de utilizar a rede Bitcoin por meio da web, transacionando normalmente como se tivesse o próprio software instalado no computador. Não há transferência de propriedade dos bitcoins do dono da carteira ao provedor de serviço de carteira online; este tampouco pode visualizar os saldos da carteira do usuário, não pode realizar transações em seu nome, não pode confiscar a sua carteira e nem mesmo pode forçá-lo a utilizar o serviço de carteira online indefinidamente[118].

Portanto, nas duas formas de custódia dos bitcoins acima descritas, pelo software Bitcoin instalado em um PC e pelo serviço de carteira online, não há um terceiro custodiando os bitcoins do proprietário. Assim, o surgimento de um substituto de bitcoin é redundante, pois as facilidades que um substituto poderia oferecer já estão incorporadas no bitcoin na sua forma mais primitiva. E a prática de reservas fracionárias seria uma impossibilidade técnica: o depositante e o depositário confundem-se; são a mesma entidade, o próprio usuário. Como poderia o dono da carteira criar substitutos de bitcoins sem lastro e transacioná-los na rede? Seria o equivalente à falsificação de bitcoins, o que é criptograficamente impossível.

Entretanto, há serviços de carteira online em que a transferência de posse e controle da carteira ocorre, sim, como é muito comum em casas de câmbio[119], ou sites que ofereçam pagamento de juros aos saldos de bitcoins lá depositados. Nesses casos, a possibilidade de surgimento de um substituto de bitcoin, ou pior, de reservas fracionárias, é maior, uma vez que o usuário do serviço não possui nem controla efetivamente a sua carteira na rede Bitcoin. Quem o faz é o provedor, em seu nome, normalmente seguindo ordens do usuário. Logo, o risco da contraparte está presente – seja de práticas ilegais, como uso indevido do seu saldo de bitcoin, seja de práticas questionáveis, como reservas fracionárias, seja de práticas insuficientes de segurança, sujeitando os usuários a ataques de *hackers* aos servidores do provedor. Grande parte dos episódios infelizes de extravio de bitcoins deve-se a este último caso.

O aparecimento da prática de reservas fracionárias com bitcoins é, portanto, bastante improvável, embora possível. Nas formas mais primitivas, o *tantundem* está a todo o instante sob posse e controle do próprio dono da carteira. Este é depositante e depositário. Mas enquanto houver serviços de carteira online em que o controle e a posse dos bitcoins são cedidos ao provedor, o risco das reservas fracionárias existe[120].

12. Outras considerações

Trataremos aqui de mais algumas preocupações frequentemente levantadas pelos críticos do Bitcoin, buscando demonstrar que carecem de fundamento, por não compreenderem a essência da moeda digital.

Eletricidade e internet não são o problema.

E quanto à dependência da eletricidade e da internet? Não seria uma enorme desvantagem ao projeto Bitcoin? Essa não é uma característica unicamente restrita ao Bitcoin, *já* vivemos nessa

dependência. É impensável que nossa economia globalizada e interconectada – bem como o sistema bancário – possa seguir inabalada na falta de energia elétrica e internet. Nesse sentido, e já endereçando outra crítica usual, acho pouco provável que governos tentem "derrubar" a internet com o objetivo de obstruir a rede Bitcoin. Aliás, considerando que governo nenhum até hoje logrou conter nenhuma rede BitTorrent[121], não me parece plausível esperar que conseguiriam causar danos irreparáveis ao maior projeto de computação distribuída do mundo (sim, Bitcoin já ultrapassou o projeto SETI, *Search for Extra Terrestrial Intelligence*).

Outros céticos argumentam que a rede poderia ser *hackeada*, corrompendo o algoritmo, alterando saldos em carteira e roubando ou falsificando bitcoins. Essa preocupação – embora compreensível – deriva do desconhecimento acerca dos atributos da rede Bitcoin. Antes de qualquer coisa, é preciso enfatizar duas inerentes características da rede: a total abertura e a transparência do sistema. Ainda que o Bitcoin tenha sido criado por um indivíduo (ou grupo de indivíduos) com certos parâmetros e regras de funcionamento, *o código fonte é completamente aberto a qualquer um* que queira verificá-lo, monitorá-lo e aprimorá-lo (este último, com o consenso de toda a comunidade). Qualquer pessoa pode acompanhar em tempo real as transações recentes, a quantidade total de bitcoins minerados, etc.

Estaríamos sugerindo que a rede Bitcoin é à prova de falhas? É lógico que não. O Bitcoin não é perfeito, e é pouco provável que não sofra alguns solavancos ao longo do seu desenvolvimento e à medida que o seu uso seja ampliado. Ainda assim, é preciso destacar que não há registro algum de ataques[122] à cadeia de blocos do sistema *(blockchain)*. Sim, é verdade que alguns sites de casas de câmbio, por exemplo, foram *hackeados* e tiveram problemas de operação, mas isso não quer dizer que a "moeda bitcoin" esteve sob ataque[123].

A concorrência das altcoins (alternate coins)

Da mesma forma, é preciso endereçar algumas das objeções mais complexas, especialmente aquelas lançadas por economistas e investidores com formidável domínio de teoria monetária. Doug Casey[124], por exemplo, alega que uma das ameaças ao Bitcoin é que não há barreiras de entradas; dessa forma, qualquer um poderia lançar sua própria moeda digital no mercado. Acabaríamos tendo, assim, diversas moedas digitais, o que inviabilizaria que uma preponderasse e viesse a tornar-se um meio de troca universalmente aceito.

Em tese, esse não é um problema exclusivo do Bitcoin. Em qualquer ambiente em que prevaleça a liberdade de escolha de moeda, qualquer um pode competir. No entanto, nessa competição, aquele meio de troca que tenha mais êxito em reduzir os custos de transação tende a sobressair-se como o mais utilizado pelos participantes. Com relação ao Bitcoin, por ter sido a primeira moeda digital, ele goza do privilégio do chamado "efeito de rede" (*network effect*). Dentro do universo de moedas digitais, Bitcoin já é a mais utilizada e com mais aderentes, portanto, ainda que uma nova moeda possa superá-la em qualidade tecnológica, a barreira de convencer usuários de Bitcoin a trocar para um concorrente é bastante grande.

Converter bitcoins em dólar, eis a questão

Já Shostak[125] alega que "Bitcoin só funciona enquanto os indivíduos souberem que podem convertê-lo em moeda fiduciária". *A priori*, não podemos determinar se isso é verdade. Essa conclusão de Shostak deriva da falaciosa ideia de que o Bitcoin é nada menos que uma "nova forma de empregar a moeda fiduciária existente". Mas se entendemos que a moeda digital é moeda propriamente dita, dinheiro de fato, perceberemos que os usuários, em realidade, podem utilizar bitcoins não com o intuito de usá-los como uma mera ferramenta de meio de pagamento, mas sim para fugir (ou liberar-se) do sistema de moeda fiduciária.

Uma vez “dentro” da rede Bitcoin, o objetivo é não ter que “voltar” às moedas locais. Sim, no momento ainda não estamos nesse estágio de evolução da rede (por causa da baixa liquidez e aceitação), mas à medida que se amplia a aceitação, não será sequer necessário fazer uso das moedas fiduciárias. Uma vez que ambos os produtores e consumidores aceitarão *receber e pagar em bitcoins*, por que convertê-los em uma moeda fiduciária que perde poder de compra constantemente?

13. Revisitando a definição de moeda

Iniciamos este capítulo definindo os termos *dinheiro* e *moeda* como o meio de troca universalmente aceito, segundo a própria definição de grande parte dos economistas da Escola Austríaca. Entretanto, e divergindo dessa definição, utilizamos a palavra moeda até o momento inclusive para qualificar o Bitcoin – moeda digital –, o que pode, com razão, suscitar questionamentos. A verdade é que a noção de moeda é vaga, é imprecisa. Especialmente no mundo moderno de moedas de papel puramente fiduciárias, a definição usual pode ser incapaz de, na prática, identificar o que seja moeda em dado tempo e lugar. Afinal de contas, moeda, hoje em dia, é o que o estado estabelece como tal. Ao economista, a definição legal de moeda é insuficiente e precária para a investigação econômica. Mas diante da realidade, não podemos ignorar seus efeitos na economia. É preciso, portanto, examinar o fenômeno detalhadamente, procurando cercar os problemas e eliminar as criações artificiais empíricas que nos impedem de deduzir logicamente a verdade científica.

Se moeda é o meio de troca universalmente aceito, quando uma mercadoria ultrapassa a linha divisória entre um mero meio de troca e passa a ser moeda? É possível encontrar, na prática, essa linha demarcando meios de troca de um lado e moeda de outro? Carl Menger, em sua obra *On the origins of money*, explica que “a teoria do dinheiro pressupõe necessariamente uma teoria da vendabilidade dos bens (*saleableness of goods*). Se compreendemos isso, deveremos ser capazes de entender como a vendabilidade quase ilimitada do dinheiro é apenas um caso especial – apresentando somente uma diferença de grau – de um fenômeno genérico da vida econômica – a saber, a diferença na vendabilidade de commodities em geral”[126]. O dinheiro é, portanto, o bem mais líquido em uma economia. Aquele pelo qual todos os outros bens são intercambiados. Mas um bem não emerge no mercado já sendo o mais líquido e mais demandado pelos indivíduos. Como elucida Menger, a escolha de uma mercadoria como meio de troca que acaba ganhando cada vez mais liquidez e prevalecendo como a mais líquida é um processo que acontece ao longo do tempo no mercado. Desse modo, e em um ciclo que se retroalimenta, os indivíduos tendem a trazer consigo ao mercado o bem mais líquido – a moeda – para realizar suas compras, reforçando e intensificando a vendabilidade do próprio bem em questão.

Ludwig von Mises, corroborando a teoria de Menger, afirma que “há uma tendência inevitável para que os bens menos comercializáveis (*marketable goods*) usados como meios de troca sejam um a um rejeitados até que, finalmente, uma única commodity permaneça, a qual é universalmente empregada como meio de troca; em uma palavra, moeda”[127]. E embora seja possível deduzir logicamente que a tendência é de somente um único bem preponderar como moeda, empiricamente a teoria pode não ser verificada – o que Mises deixa perfeitamente claro ao constatar que “este estágio de desenvolvimento no uso de meios de troca, o emprego exclusivo de um único bem econômico, não está ainda completamente alcançado”[128].

Se dinheiro é o meio de troca universalmente aceito, em grande parte da história monetária

nem mesmo o ouro poderia ser qualificado como tal, porque a prata esteve quase sempre ao seu lado sendo empregada como meio de troca, universalmente aceita, e com uma liquidez praticamente tão alta como a do ouro – salvo casos em que soberanos legislavam contra o uso de um ou o outro metal. E por que o ouro jamais prevaleceu como a única moeda – estágio ainda não atingido por nenhum bem, conforme apontado por Mises? Possivelmente, dentre outras razões, porque lhe falta uma perfeita divisibilidade em face de sua substancial escassez. Isso significa que há um alto valor por unidade do metal[129]. E, é claro, há um limite físico pelo qual o metal pode ser fracionado. Devido a essa razão, a prata, mais abundante e com propriedades físico-químicas muito similares às do ouro, acabou por ser um ótimo meio de troca para compras de menor valor ao longo da história.

Diante da imprecisão conceitual de moeda, Murray N. Rothbard sugere uma forma de contornar o problema em sua obra seminal, *Man, economy and state*:

> Uma commodity que passa a ter uso generalizado como meio de troca é definida como sendo uma moeda. É evidente que, enquanto o conceito de "meio de troca" é preciso, e uma troca indireta pode ser distinguida de uma direta, o conceito de "moeda" é menos preciso. O instante em que um meio de troca passa a ter uso "comum" ou "geral" não é estritamente definível, e se um meio de troca é ou não dinheiro, somente pode ser decidido pela investigação histórica e pelo julgamento do historiador. Entretanto, visando à simplificação, e como vimos que há um grande ímpeto no mercado para um meio de troca tornar-se moeda, de agora em diante, nos referiremos a todos os meios de troca como moedas.[130]

Rothbard, na verdade, apenas evita lidar com o problema, pois o conceito de moeda permanece envolto de imprecisão. Levada ao extremo, essa definição simplificada pode conduzir-nos a conclusões claramente descabidas. Imaginemos o exemplo de um incorporador que vende um apartamento e concorda em receber como pagamento 80% do valor do imóvel em dinheiro e o restante em troca de um automóvel (dação em pagamento) – ainda que o vendedor não tenha interesse algum em utilizar o automóvel e busque desfazer-se do bem o quanto antes. Nesse caso, por ter servido como um meio de troca, poderíamos qualificar o automóvel como moeda? Claramente, não. É bastante provável que o futuro comprador do automóvel o adquirirá não para revendê-lo, mas sim para usá-lo, consumi-lo. Por mais que o automóvel possa servir como meio de troca em dada transação, seu destino principal é ser consumido, é um bem de consumo (ou produção, dependendo do usuário), e não um meio de troca[131] [132].

A teoria monetária desenvolvida pelos economistas da Escola Austríaca sustenta que há uma tendência inevitável para uma única moeda prevalecer no mercado, sendo esta a universalmente aceita. Empiricamente, essa teoria foi ilustrada por mais de 2.000 anos de história repletos de registros em que o ouro, e em menor medida a prata, imperou como a moeda escolhida pelo mercado. Essa era a realidade, inclusive, da época em que Menger e Mises desenvolveram suas teorias monetárias.

A verdade é que o dinheiro global sempre foi o ouro e a prata. Mas nem sempre eram moedas ou barras de ouro aquilo que os indivíduos davam em troca em uma transação. Especialmente com a intensificação da divisão internacional do trabalho, o aprofundamento do sistema bancário e após a Revolução Industrial, mais rara era a prática de as pessoas carregarem metais consigo. O que circulava eram as moedas nacionais – *currency*[133], em inglês –, meras representações (substitutos de dinheiro) da moeda propriamente dita, o ouro. As moedas nacionais eram, historicamente, definições de massa do metal precioso; eram as unidades monetárias de cada

estado-nação.

Na língua portuguesa, não temos uma tradução exata para *currency*. Poderíamos traduzir como moeda corrente ou moeda nacional. Mas também se traduz simplesmente como moeda, da mesma forma que *money*. Posto que hoje em dia os termos realmente se confundem, é necessário ressaltar a distinção entre os dois. Uma moeda de ouro, dinheiro no sentido econômico do termo, pode receber diferentes denominações, dependendo do estado que a cunha. Tomemos o exemplo do Império Alemão. Tendo sido o *Goldmark* definido por lei a 2.790 marcos o quilo do ouro, no fim do século XIX, a moeda (peça metálica) de 5 *Goldmark* pesava aproximadamente 2 gramas e continha 1,8 grama de ouro. A *currency* (a moeda nacional) era o marco alemão, o ouro, o dinheiro propriamente dito. A forma mais primitiva de depreciar a moeda consistia em misturar algum metal mais abundante e de inferior qualidade, diluindo o conteúdo do ouro, mas mantendo o peso e a denominação oficial (por ex.: 5 marcos pesando 2 gramas). A *currency* era assim desvalorizada.

Valores maiores exigiam o uso de barras ou lingotes de ouro com maior massa e de difícil transporte, tarefa facilitada pelas cédulas de papel emitidas pelos governos e/ou bancos centrais. Assim, a moeda nacional era impressa em uma cédula com certa denominação (por ex.: a nota de 100 marcos no final do século XIX, equivalente a 36 gramas de ouro), a qual representava uma quantidade específica do metal precioso, podendo ser resgatada em espécie quando assim solicitado pelo portador a algum banco depositário. A moeda nacional (*currency*), assim, era separada da moeda propriamente dita, o ouro. A moeda nacional era uma representação do metal que poderia ser convertida em ouro quando demandado pelo proprietário da cédula de papel. Isso nada mais é do que a definição do padrão-ouro clássico; a paridade do ouro era promulgada em lei, e a moeda nacional circulava e era aceita independentemente de qualquer lei de curso forçado, pois a *currency* era resgatável em ouro, e os bancos centrais de fato obedeciam à lei. Até o início da Primeira Guerra Mundial, essa era a ordem monetária do Ocidente[134]. O ponto a ser compreendido aqui é que, mesmo no padrão-ouro clássico em que as cédulas de banco eram, em sua maior parte, lastreadas em ouro, cada vez menos o metal circulava, sendo a maioria das trocas de mercado realizadas com cédulas de papel, a moeda nacional.

Com a abolição do padrão-ouro pelos estados, o ouro deixou de ser moeda propriamente dita – por força de lei, é verdade –, e a moeda nacional (*currency*) passou a ser o dinheiro de fato, ou, em uma palavra, papel-moeda. Por essa razão, os termos ingleses *money* e *currency* são hoje sinônimos, embora historicamente seja possível observar a distinção entre os dois. Quando esse processo de remoção do vínculo ao ouro estava se desenrolando, a maioria dos economistas encarava a realidade como uma condição de total anomalia monetária. Como os cidadãos transacionariam com uma moeda nacional inconversível? A moeda de fato, o ouro, estava sendo proibida? Tendo a moeda se transformado em papel-moeda sem lastro, como classificá-la segundo a teoria monetária? O dólar americano seria moeda? E francos suíços? Especialmente em cidades e mercados fronteiriços, onde duas ou mais moedas nacionais costumam circular, como determinar qual papel-moeda é ou não dinheiro? Todavia seja uma situação anômala, o fato é que vivemos em um mundo onde o papel-moeda é a moeda propriamente dita, e o ouro, que foi moeda ao longo de milênios, foi relegado ao posto de ativo financeiro e reserva de valor, mas com pouquíssimo uso como meio de troca. No mundo de Menger e Mises, ouro era a moeda global. Atualmente, temos quase duzentas moedas nacionais sem qualquer lastro material circulando em diversas jurisdições. Se moeda é o meio de troca universalmente aceito, hoje o que é moeda no sentido estritamente econômico do termo?

De acordo com essa definição, não há uma clara distinção entre o que é ou não moeda – ainda

que a lei estabeleça claramente o que é moeda em cada jurisdição. O que encontramos é, ao contrário, "um *continuum* em que objetos com vários graus de liquidez, ou com valores que podem oscilar independentemente, se confundem um com o outro quanto ao grau em que funcionam como dinheiro"[135]. Em um mundo com dezenas de papéis-moedas circulando, essa é a incontestável realidade.

Vivendo intensamente os primeiros anos de moedas nacionais puramente fiduciárias e inconversíveis – a partir de 1971 com o fim da conversibilidade do dólar em ouro –, F.A. Hayek percebeu nitidamente essa imprecisão na definição de moeda. Em *Desestatização do Dinheiro*, ele observa que:

> Sempre considerei útil explicar a meus alunos que é pena qualificarmos o dinheiro como substantivo, e que seria mais útil para a compreensão dos fenômenos monetários se 'dinheiro' fosse um adjetivo descrevendo uma propriedade que diferentes objetos poderiam possuir, em graus variados. 'Moeda corrente' (*currency*) é, por esse motivo, uma expressão mais adequada, uma vez que objetos podem ter curso (*have currency*), em graus variáveis, e em diferentes regiões ou setores da população.[136]

Moeda, então, é mais bem entendida como uma qualidade de uma mercadoria de servir como um meio de troca, como um bem que é intercambiado no mercado e circula de mão em mão sem jamais, ou por um longo período, ser consumido de fato. Tal qualidade é potencializada ou debilitada por atributos variados intrínsecos a uma mercadoria – escassez, durabilidade, homogeneidade espacial e temporal, divisibilidade, maleabilidade, transportabilidade, etc. – e atributos "artificiais" conferidos por influências externas e estrangeiras à natureza da mercadoria – leis estatais de curso forçado, restrições legais de uso, etc. O conjunto desses atributos, endógenos e exógenos, impacta diretamente na qualidade monetária de uma mercadoria. E embora, a priori, pressupõe-se que qualquer mercadoria poderia ser empregada como meio de troca, há uma tendência inevitável de sobressaírem-se os bens que apresentarem os melhores atributos elencados acima. Esses bens, dentre os diversos usos que oferecem, tenderão a ser majoritariamente utilizados como meio de troca e valorados, em maior medida, pelos serviços monetários que proveem do que pelos serviços de consumo ou produção que podem também prover.

Logo, diferentes bens monetários podem se diferenciar uns dos outros em duas dimensões distintas e ora relacionadas, liquidez (aceitação) e estabilidade (volatilidade ou expectativa de valor).[137] Em certa região e em dado momento, diferentes bens monetários podem ser empregados com graus distintos de liquidez e estabilidade, sendo possível que, na mesma região, em outras épocas, distintos bens circulem como meio de troca, ou, até mesmo, noutras regiões, mas na mesma época, ainda outros bens possam ser utilizados como meio de troca.

Diante do exposto acima, definir moeda (ou dinheiro) como meio de troca universalmente aceito pode tornar o substantivo uma teoria inalcançável na prática, sendo jamais verificada empiricamente. Em virtude disso, há duas alternativas. Primeiro, nos atermos a essa definição comumente aceita, sendo obrigados, então, a matizar o conceito sempre que o empregarmos para estudar os fenômenos monetários da realidade – qual o meio de troca *mais líquido, em certo país, no dia de hoje*?[138] Ainda que plenamente possível, adotando essa postura permaneceremos com esse nível de imprecisão, dependendo substancialmente da investigação histórica e do julgamento do historiador a cada instante.

Por essas razões, acreditamos ser apropriada uma segunda alternativa. Propomos um refinamento na definição de moeda, visando remover o máximo possível de imprecisões

remanescentes. Em vez de definirmos moeda como o meio de troca universalmente aceito, talvez o mais razoável seja a seguinte forma: ***moeda é qualquer bem econômico empregado indefinidamente como meio de troca***, independentemente de sua liquidez frente a outros bens monetários e de seus possíveis usos alternativos. Ressalte-se, sobretudo, que há uma tendência inevitável a que somente uma moeda prevaleça no mercado, sendo ela então a mais líquida, ou, até mesmo, a única moeda – admitindo que, na prática, uma única moeda seja algo que, talvez, jamais será alcançado.

É inegável que substituímos uma imprecisão – como identificar qual o meio de troca mais líquido para poder descobrir, então, qual é a moeda? – por outra – como apontar a partir de qual momento um bem passa a ser usado indefinidamente como meio de troca, tornando-se, assim, moeda? Entretanto, esta depende menos do julgamento subjetivo de cada historiador, sendo, assim, menos inexata do que aquela. A definição de moeda aqui proposta evita que caiamos nas áreas cinzentas, como ocorre naquelas regiões onde mais de uma moeda circula normalmente – cidades fronteiriças ou estados famosos pela livre circulação do dólar americano em paralelo à moeda nacional –, em que seria praticamente impossível identificar a moeda seguindo a definição de meio de troca comumente aceito. Resta claro que, nesses casos, tanto o dólar quanto o peso uruguaio, por exemplo, são moedas, embora na maioria dos municípios do Uruguai seja a moeda nacional a mais líquida.

Vale ressaltar que, assim como o mercado em geral é um processo dinâmico e competitivo, há concorrência no mercado de moedas, e nada garante que uma moeda muito líquida em dado instante e lugar não seja substituída por outra, em um processo competitivo, podendo até mesmo ser desconsiderada, no futuro, como uma moeda propriamente dita, passando a ser apenas uma mercadoria que, no passado, já foi empregada como bem monetário.

Logicamente, da definição de moeda aqui proposta – *qualquer bem econômico empregado indefinidamente como meio de troca* –, derivam algumas conclusões importantes. Primeiro, o ouro, atualmente, não é moeda, mas sim um ativo financeiro usado como reserva de valor. Desconheço empresas ou até mesmo indivíduos que aceitem o metal como meio de troca em transações comerciais. Certamente existem, mas em quantidade desprezível. Hoje em dia, o proprietário de uma barra de ouro dificilmente conseguirá usá-la como meio de troca; deverá, na realidade, converter o ouro em alguma moeda (dólar, euros, reais, etc., com grande dificuldade, dependendo da região e da forma do ouro em posse), para então poder comprar algo com moeda de fato. O ouro seria mais bem enquadrado na definição misesiana de moeda secundária, em que um bem altamente líquido precisa ser convertido em moeda antes de ser usado em alguma troca.

Segundo, e por fim, seria o bitcoin uma moeda? Sim, pois já existem diversas empresas e indivíduos transacionando com bitcoins mundo afora, com distintos graus de liquidez dependendo da região. Vale destacar que o número dos que com a moeda digital transacionam tem crescido constantemente. Contudo, poder-se-ia argumentar que ainda há muita demanda puramente especulativa ou como reserva de valor, e não como meio de troca. Nenhuma das alegações, porém, invalida o fato de a moeda digital já ser um meio de troca. A grande verdade é que há especulação em qualquer mercado de moeda. Aliás, as moedas são a principal classe de ativos em termos de volumes negociados, sendo responsáveis por mais de US$ 5 trilhões de dólares de volume transacional médio diário nos mercados cambiais (*currency* ou *foreign exchange markets*)[139]. A diferença entre a especulação de moedas tradicionais e a de moedas digitais é apenas uma questão de liquidez e desenvolvimento dos mercados financeiros tradicionais e de derivativos – daí, também, boa parte da razão da alta volatilidade do bitcoin. Reserva de valor, entretanto, é meramente um aspecto temporal da função primordial de meio de

troca[140]. Devido à expectativa de futura manutenção ou apreciação de valor da moeda digital, muitos usuários podem decidir manter encaixes em bitcoins por um prazo mais alongado do que o fariam com moedas convencionais. Mas, ainda assim, com o objetivo – e a crescente possibilidade – de usá-los como bem monetário no futuro. Bitcoin é, portanto, uma moeda, um bem econômico empregado indefinidamente como meio de troca, embora com liquidez inferior à da maior parte das moedas fiduciárias nacionais neste instante da história[141].

Que essa definição de dinheiro aqui sugerida não seja encarada como uma tentativa de reinventar a teoria da moeda, pois não o é. Procuramos meramente oferecer um aprimoramento da *definição* usual de moeda, especialmente em face da realidade atual em que as antigas moedas globais – ouro e prata – desempenham praticamente nenhuma função monetária e o que temos, de fato, são quase duzentas moedas nacionais circulando pelo mundo como meio de troca, sem qualquer lastro além da confiança de seus bancos emissores. Além disso, a teoria monetária desenvolvida por Mises já contempla o uso de diversos tipos de moeda no mercado:

> A teoria do dinheiro deve levar em consideração tudo que está implícito no funcionamento de diversos tipos de moeda lado a lado. Somente onde suas conclusões são improváveis de serem afetadas de uma forma ou de outra, podemos proceder a partir da suposição de que um único bem é empregado como meio de troca comum. Nos demais casos, a teoria deve considerar o uso simultâneo de diversos *meios de troca*. Negligenciar isso seria esquivar-se de uma das tarefas mais difíceis.[142] (ênfase nossa).

Da mesma forma, e mais ciente da imprecisão na definição de moeda e de sua irrelevância para a teoria monetária, Mises elucida, na sua obra Ação Humana, que:

> Um meio de troca que seja de uso comum é denominado de moeda. A noção de moeda é vaga, uma vez que sua definição implica o emprego da expressão “uso comum”, que é igualmente vaga. Existem situações nas quais se torna difícil definir se um meio de troca é ou não de uso “comum” e se pode ser denominado de moeda. Mas esta imprecisão na caracterização da moeda não afeta, de forma nenhuma, a exatidão e a precisão exigidas pela teoria praxeológica. Porque tudo o que possa ser predicado sobre moeda é válido para qualquer meio de troca. Resulta, portanto, irrelevante preservar o termo tradicional teoria da moeda, ou substituí-lo por outra denominação. A teoria da moeda foi e continua sendo a teoria da troca indireta e dos meios de troca.[143]

Em conclusão, visando exclusivamente uma maior exatidão dos termos, propomos aqui denominar de moeda o que muitos economistas provavelmente prefeririam qualificar apenas como meio de troca.

14. Meio de troca, reserva de valor e unidade de conta

As funções comumente atribuídas ao dinheiro são as de servir como i) meio de troca, ii) reserva de valor e iii) unidade de conta. Porém, as três funções não emergem instantaneamente no momento em que um bem passa a ser utilizado como meio de troca. Na verdade, facilitar as trocas, desempenhar a função de meio de troca é *a função* da moeda e, como elaborado acima, é como a moeda deve ser, inclusive, definida.

Um bem que ganha crescente liquidez no mercado tende a ser estocado, ou entesourado, como reserva de valor, de riqueza, para ser usado no comércio futuramente, quando será, então,

empregado como meio de troca. Decorre, assim, que a moeda é também usada como preservação de poder de compra futuro. Isso nada mais é do que a função primordial de meio de troca manifestando-se no tempo e no espaço. Logicamente, a moeda não é único bem escolhido como reserva de valor; outros ativos podem desempenhar esse serviço, como imóveis e metais preciosos. Mas ambos, com graus de liquidez claramente distintos, não são usados como meio de troca – o ouro já foi por milênios, mas atualmente é um ativo financeiro de proteção, de preservação de valor. O que um indivíduo decide entesourar como reserva de valor dependerá de suas necessidades monetárias frente aos seus dispêndios futuros e da liquidez e expectativa de valor das diferentes moedas e ativos disponíveis no mercado. Servir como reserva de valor é, portanto, uma função secundária do dinheiro.

A terceira função comumente atribuída à moeda – unidade de conta – também é derivada de seu uso como meio de troca. À medida que a liquidez de um bem monetário aumenta e este passa a circular como a principal moeda em uma economia, os indivíduos tenderão a precificar os produtos e serviços e a realizar o cálculo econômico em função dessa moeda. Talvez resida aqui o marco de uma moeda amplamente aceita e desenvolvida, quando ela passa a ser usada não somente como meio de troca, mas também como a unidade de conta geral.

É a intervenção estatal no âmbito monetário, porém, a causa de genuínas anomalias econômicas. A interferência dos governos na moeda pode causar sérios danos à saúde monetária da economia, sendo capaz de separar por completo as três funções de um meio de troca usado em um país. É a inflação, a desvalorização da unidade monetária, o que leva indivíduos a buscar refúgios em moedas mais seguras e estáveis, como ocorria frequentemente no Brasil de décadas passadas, em que o dólar era entesourado pelos cidadãos e a moeda corrente nacional era gasta o mais rapidamente possível. A função de meio de troca era assim divorciada da função de reserva de valor e de unidade de conta. Primeiro, porque os cidadãos mantinham encaixes na moeda nacional somente para o estritamente necessário no curto prazo. E segundo, porque quando a moeda nacional perde valor de forma intensa e rápida, o cálculo econômico é seriamente debilitado, quando não impossibilitado.

No Brasil passado, a combinação de leis de curso forçado e da alta inflação da oferta de moeda nacional conduziu a um espetáculo de horror em questões monetárias. Dinheiro físico (papel-moeda) era usado nas transações do dia a dia, enquanto o dólar (papel-moeda) era entesourado nos lares. Os preços e o cálculo econômico eram realizados na moeda nacional, mas, desde cedo, com o suporte fundamental da indexação, que permitia um mínimo de racionalidade nas decisões econômicas e de preservação do poder de compra. E, dependendo dos mercados, o próprio dólar era a unidade de conta utilizada, ato comum no setor imobiliário, por exemplo. De fato, sem a coerção estatal, uma anomalia monetária dessa magnitude seria rapidamente evitada; os cidadãos migrariam ao uso de moedas seguras e estáveis tão logo quanto possível. Uma moeda nacional inflacionada pelo estado, que perde poder aquisitivo constantemente, dificilmente mantém as propriedades de reserva de valor e unidade de conta por si só. E a rapidez com que tal condição é verificada na prática é diretamente proporcional à intensidade da inflação.

Mas o que ocorreria com uma moeda que ganha poder de compra ao longo do tempo – como tem sido o bitcoin? Como seriam afetadas as funções de reserva de valor e unidade de conta? Mises defende que:

> Para o bom funcionamento do cálculo econômico, basta evitar flutuações grandes e abruptas na oferta de dinheiro. O ouro e, até meados do século XIX, a prata, atenderam muito bem às necessidades do cálculo econômico. As variações na relação entre a oferta

> e a demanda destes metais preciosos e as consequentes alterações no poder de compra foram tão lentas que o cálculo econômico dos empresários podia desprezá-las sem correr o risco de grandes desvios[144].

Pelo lado da oferta, o protocolo do Bitcoin assegura um crescimento da quantidade de bitcoins determinado e conhecido por todos. E independentemente de qualquer evento, a oferta monetária seguirá aumentando nesse ritmo pré-estabelecido. Pelo lado da demanda, porém, ainda há grandes oscilações, daí a razão de tamanha volatilidade, nesses primeiros anos, no preço do bitcoin, e, por isso, a precificação dos bens e serviços adquiridos por bitcoin permanecem sendo efetuadas na moeda corrente. Felizmente, a demanda, embora volátil, tem crescido no longo prazo. O mesmo pode ser afirmado sobre o preço do bitcoin.

A verdade é que o bitcoin está passando por um processo de monetização, e enquanto a volatilidade perdurar, dificilmente será adotado como unidade de conta. O aumento de sua liquidez e aceitação, porém, pode definitivamente fazer com que o bitcoin seja não apenas um meio de troca e um ativo para preservação de riqueza, mas também a moeda em função da qual os produtos e serviços são precificados e com a qual é realizado o cálculo econômico. Um sinal de que o bitcoin atingiu um estágio avançado de desenvolvimento será o momento em que a moeda digital for um meio de troca, uma reserva de valor *e uma unidade de conta*.

15. Conclusão

Atentando à advertência de Mises, buscamos, neste capítulo, nos ater à essência do Bitcoin, não deixando que a mera aparência nos impedisse de compreender um fenômeno fundamentalmente similar a outras formas de dinheiro como as conhecemos.

O surgimento do Bitcoin em nada contraria o teorema da regressão de Mises, ao contrário, é a mais recente ilustração histórica do enunciado praxeológico acerca da origem do dinheiro. Assim, como economistas, estamos presenciando em tempo real o nascimento e a formação de uma moeda totalmente globalizada, apolítica, sem fronteiras e livre. Além disso, esse processo se desenrola diante de nossos olhos com um vasto registro histórico que se avoluma a cada novo dia na vida da moeda digital. Um feito inédito, sem dúvida alguma.

Apesar da aparência unicamente digital, as atuais formas de dinheiro assemelham-se em muito ao Bitcoin. A maior parte da massa monetária no mundo moderno manifesta-se de forma intangível; nosso dinheiro já é um bem incorpóreo, uma característica que em nada nos impede de usá-lo diariamente. Não obstante as similitudes, o Bitcoin introduz inovações antes inconcebíveis pela mente humana. Sua natureza totalmente descentralizada; o compartilhamento de um registro público, único e universal por todos os usuários; a capacidade de transferência de fundos instantânea a qualquer parte do globo terrestre; e o fato de prescindir de um terceiro fiduciário para transacionar fazem do Bitcoin uma façanha da civilização. Além do mais, tais atributos fazem com que o Bitcoin, como sistema monetário, incorpore as principais qualidades das formas de moedas existentes – como a escassez relativa do ouro e a transportabilidade do papel-moeda –, aperfeiçoando suas principais fraquezas – como a dificuldade de transportar e estocar metais preciosos ou a ilimitada produção de papel-moeda. Bitcoin é, simplesmente, uma forma de dinheiro superior a todas as demais.

Como moeda, poderá o Bitcoin ampliar sua liquidez e sua relevância no comércio internacional? No que depende da teoria econômica, não há nada que o previna de alcançar tal

posto. Potencial para tanto, o Bitcoin seguramente tem. No que depender da livre ação humana, da função empresarial dos homens, é possível que a adoção do Bitcoin seja ampliada, bem como sua liquidez. Porque, como diz Menger:

> Só podemos entender por completo a origem do dinheiro se aprendermos a visualizar o estabelecimento do procedimento social que estamos tratando, como o resultado espontâneo, a resultante não premeditada, de certos esforços individuais dos membros de uma sociedade, os quais se empenharam, pouco a pouco, a discriminar os diferentes graus de vendabilidade de cada commodity.[145]

E, além de discriminar dentre as mercadorias que apresentavam a maior liquidez, a criatividade humana, identificando propriedades que tornariam um bem um melhor meio de troca, sempre tratou de aperfeiçoar tais mercadorias de modo a aumentar a liquidez de um bem já bastante comercializável. Exatamente com esse intuito, cunhavam-se barras ou moedas de ouro, porque transacionar com ouro em sua forma bruta seria muito complicado, impedindo uma maior aceitação no mercado.

Estamos testemunhando esse mesmo processo com o Bitcoin. As ações espontâneas de alguns membros da sociedade criaram uma forma de moeda inovadora e superior à que hoje conhecemos. É plausível, portanto, vislumbrar a intensificação desse processo, em que o dinamismo do mercado e a inata criatividade do ser humano descobrirão formas de aumentar a liquidez do Bitcoin.

Assim como o ouro e prata são consideradas “moedas naturais” – cuja emersão como meio de troca geralmente usado foi um processo espontâneo do livre atuar dos indivíduos no mercado –, podemos, igualmente, definir o Bitcoin como uma moeda natural, que passa a ser usada pela cooperação voluntária dos membros de uma sociedade, provendo apoio mútuo sem qualquer violação dos direitos de propriedade de outrem[146]. Amiúde, estados solaparam as moedas naturais em benefício próprio. Mas a natureza descentralizada da moeda digital impõe um revés ao ímpeto intervencionista estatal. Com certeza, é um ponto de inflexão na história monetária mundial, cujos desdobramentos só podemos especular.

Rodapé

68 De *cataláxia*: a teoria da economia de mercado, isto é, das relações de troca e dos preços. Analisa todas as ações com base no cálculo monetário e rastreia a formulação de preços até a sua origem, ou seja, até o momento em que o homem fez sua escolha. Explica os preços de mercado como são, e não como deveriam ser. As leis da cataláxia não são julgamentos de valor; são exatas, objetivas e de validade universal.
69 MISES, Ludwig von Mises. The Theory of Money and Credit. New Haven: Yale University Press, 1953. p. 462.
70 Ibid., p. 468.
71 MISES, 2010, p. 125.
72 Ibid., p. 125.
73 Disponível em: <https://bitcointalk.org/index.php?topic=91806.msg1012234#msg1012234>. Acesso em: 22 dez. 2014.
74 MISES, 2010, p. 156-157.
75 As futuras e possíveis aplicações do Bitcoin serão tratadas com mais detalhes no último capítulo do livro.
76 MISES, Ludwig von. Theorie des Geldes und Umlaufsmittel. Munique:
Verlag von Duncker & Humblot, 1924.
77 GRAF, Konrad S. Bitcoins, the regression theorem, and that curious but unthreatening empirical world, 27 fev. 2013. Disponível em: <http://konradsgraf.com/blog1/2013/2/27/in-depth-bitcoins-the-regression-theorem-and-that-curious-bu.html>. Acesso em: 22 dez. 2013.
78 Destacando o fato de que a moeda despertou a curiosidade de pensadores ao longo da história da humanidade, Carl Menger ressalta precisamente esse ponto. Referindo-se ao ouro ou moedas metálicas, Menger pergunta-se: “Qual a

natureza destes pequenos discos ou documentos, que eles próprios parecem não servir nenhuma função útil e que, ainda assim, e em contradição com o resto da experiência, passam de uma mão a outra em troca das commodities mais úteis, pelos quais todo mundo está prontamente disposto a entregar seus produtos? A moeda é um membro orgânico do mundo das commodities ou é uma anomalia econômica?” MENGER, Carl. On the Origins of Money. Economic Journal, volume 2, 1892. p. 239.

79 Disponível em: <https://en.bitcoin.it/wiki/History#2010>. Acesso em: 22 dez. 2013.

80 MISES, 1953, p. 121.

81 MISES, 2010, p. 126.

82 MISES, 2010, p. 125.

83 TUCKER e KINSELLA. Goods, Scarce and Nonscarce. Mises Daily, Auburn: Ludwig von Mises Institute, 25 ago. 2010. Disponível em: <http://mises.org/daily/4630/>. Acesso em: 22 dez. 2013.

84 GRAF, Konrad S. The sound of one bitcoin: Tangibility, scarcity, and a “hard-money” checklist, 19 mar. 2013. Disponível em: <http://konradsgraf.com/blog1/2013/3/19/in-depth-the-sound-of-one-bitcoin-tangibility-scarcity-and-a.html>. Acesso em: 22 dez. 2013.

85 BÖHM-BAWERK, Eugen. Whether Legal Rights And Relationships Are Economic Goods, Shorter Classics Of Eugen Von Böhm-Bawerk Volume I, South Holland: Libertarian Press, 1962.

86 Não discorreremos em detalhe sobre todos os efeitos do sistema de reserva fracionária. Para uma breve introdução, ver capítulo anterior ou, para aqueles que desejam aprofundar-se no tema, ver HUERTA DE SOTO, Jesús. Moeda, crédito bancário e ciclos econômicos. São Paulo: Instituto Ludwig von Mises Brasil, 2012.

87 A moeda bancária faz parte dos chamados “meios fiduciários”. Seguindo a definição de Mises, “meio fiduciário é todo substituto perfeito de dinheiro (depósitos, cédulas de banco, etc.) não respaldado por dinheiro mercadoria”. MISES, 2010.

88 Os primeiros indícios da prática de reserva fracionária remontam à Grécia Antiga. Ver capítulo II, HUERTA DE SOTO, 2012.

89 Usando os dados mais recentes, na data de 29 de novembro de 2013, a relação foi calculada dividindo os depósitos à vista contidos no agregado monetário M1 pelo próprio M1 (papel-moeda + depósitos à vista = M1).

90 Criadas pelo empresário americano Mike Caldwell, as moedas Casascius funcionam como uma espécie de “cartão-presente” de bitcoins. Há uma chave privada associada à moeda, que está vinculada a uma chave pública (endereço Bitcoin) e a uma quantidade determinada de bitcoins no *blockchain*. Um holograma protege a chave privada e pode ser removido para “resgatar” os bitcoins online.

91 ŠURDA, Peter. Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold? Diploma Thesis, Wirtschaftsuniversität Wien, 2012. Disponível em: <http://dev.economicsofbitcoin.com/mastersthesis/mastersthesis-surda-2012-11-19b.pdf>. Acesso em: 15 abr. 2013.

92 GRAF, 2013.

93 SHOSTAK, Frank. The Bitcoin Money Myth. Mises Daily, Auburn: Ludwig von Mises Institute, 17 abr. 2013. Disponível em: <http://mises.org/daily/6411/The-Bitcoin-Money-Myth>. Acesso em: 22 dez. 2013.

94 MISES, 1953, p. 62.

95 GRAF, 2013.

96 Retomaremos essa questão na seção 13 deste capítulo.

97 GERTCHEV, Nikolay. The Money-ness of Bitcoins. Mises Daily, Auburn: Ludwig von Mises Institute, 4 abr. 2013. Disponível em: <http://mises.org/daily/6399/The-Moneyness-of-Bitcoins>. Acesso em: 22 dez. 2013.

98 MATONIS, Jon. How Cryptocurrencies Could Upend Banks’ Monetary Role. The Monetary Future, 15 mar. 2013. Disponível em: <http://themonetaryfuture.blogspot.com.br/2013/03/how-cryptocurrencies-could-upend-banks.html>. Acesso em: 22 dez. 2013.

99 GRAF, 2013.

100 REISMAN, George. Deflação, prosperidade e padrão-ouro. Instituto Ludwig von Mises Brasil, 16 ago. 2010. Disponível em: <http://mises.org.br/article.aspx?id=752>. Acesso em: 25 dez. 2013.

101 Que não levemos esse argumento ao extremo; é claro que apenas um grama de ouro não serviria como oferta monetária a uma economia.

102 Neste momento (janeiro de 2014), já é necessário transacionar em frações de bitcoins, uma vez que o preço de mercado tem oscilado ao redor de 900 dólares.

103 Disponível em: <http://www.bcb.gov.br/?PADMONET>. Acesso em: 26 dez. 2013.

104 O termo hiperdeflação não é correto, pois nesse caso não há uma contração abrupta da oferta monetária (o que seria o exato inverso de hiperinflação), apenas uma oferta monetária quase estática em que a demanda pela moeda cresce constante e paulatinamente ao longo do tempo. Utilizamos o termo aqui visando unicamente contrastar a ideia.

105 Para um excelente resumo da evolução dos preços do bitcoin, ver GRAF, Konrad S. On The Origins Of Bitcoin, 3 dez. 2013. Disponível em: <http://konradsgraf.squarespace.com/storage/On%20the%20Origins%20of%20Bitcoin%20Graf%2003.11.13.pdf>. Acesso em: 5 dez. 2013.

106 Janeiro de 2014.

107 Disponível em:

<http://www.reddit.com/r/subredditofthedaycomments/1akod6march_19th_2013_rbitcoin_currency_of_the_future/>. Acesso em: 26 dez. 2013.

108 Fato ocorrido precisamente no dia 15 de agosto de 1971, quando Richard Nixon, então presidente dos Estados Unidos, suspendeu qualquer conversibilidade do dólar em ouro.

109 Ex-presidente do Federal Reserve Ben Bernanke, durante discurso em Jackson Hole, Wyoming, EUA, declarou que, desde o início da crise de 2008, “os banqueiros centrais estão no processo de aprendendo com a prática”. Ver BERNANKE, Ben, Monetary Policy since the Onset of the Crisis, Federal Reserve, 31 ago. 2012. Disponível em: < http://www.federalreserve.gov/newsevents/speech/bernanke20120831a.htm>. Acesso em: 27 dez. 2013.

110 PIERRE. The Bitcoin Central Bank’s Perfect Monetary Policy. The Mises Circle, 15 dez. 2013. Disponível em: <http://themisescircle.org/blog/2013/12/15/the-bitcoin-central-banks-perfect-monetary-policy/>. Acesso em: 27 dez. 2013.

111 O adjetivo assintótico deriva de “assíntota”, que em geometria significa uma reta que é tangente de uma curva no infinito, ou seja, que, prolongada indefinidamente, se aproxima cada vez mais do ponto de tangência de uma curva, mas sem jamais encontrá-lo. Ou, dito de outra forma, que se aproxima de um limite, porém, nunca o alcança.

112 Ibid.

113 Ver próxima seção, sobre possibilidade de reservas fracionárias no Bitcoin.

114 A Trindade Impossível é um dilema em economia internacional que afirma que é impossível uma autoridade monetária adotar as três seguintes políticas simultaneamente: câmbio fixo, liberdade no fluxo de capitais e uma política de juros independente.

115 HUERTA DE SOTO, 2012, p. 11.

116 Entre os economistas da Escola Austríaca, há um vigoroso debate quanto à alegação de as reservas fracionárias constituírem ou não uma fraude legal. Para o propósito do presente livro, essa discussão é desimportante.

117 Ver capítulo II.

118 As chaves privadas são guardadas pelo *browser* do usuário, e não pelos servidores do provedor de serviço. Para entender a tecnologia envolvida que possibilita tal façanha, ver site da empresa Blockchain. Disponível em: <https://blockchain.info/pt/wallet/how-it-works>. Acesso em: 27 dez. 2013.

119 Nesses casos, a chave privada fica em posse e controle do provedor de serviço, ainda que esteja associada a um usuário devidamente logado e registrado no site do provedor.

120 No início de fevereiro de 2014, clientes da casa de câmbio Mt.Gox vivenciaram possivelmente esse problema. Com enormes dificuldades técnicas para honrar as retiradas de bitcoins solicitas pelos depositantes, a empresa suspendeu temporariamente todo e qualquer resgate da moeda digital. Até o momento da impressão deste livro, o caso permanecia pendente de resolução.

121 Goldmoney Podcast. Disponível em: <http://www.goldmoney.com/podcast/jon-matonis-on-bitcoin-and-crypto-currencies.html>. Acesso em: 20 mai. 2013.

122 Disponível em: <https://en.bitcoin.it/wiki/myths#Bitcoin_was_hacked>. Acesso em: 10 nov. 2013.

123 Seria como afirmar que o real foi atacado porque alguns bandidos roubaram o cofre da agência da Av. Paulista do Banco do Brasil.

124 DUNCAN, Andy. The Great Gold vs. Bitcoin Debate: Casey vs. Matonis. Lew Rockwell, 15 abr. 2013. Disponível em: <http://lewrockwell.com/orig11/duncan-a4.1.1.html>. Acesso em: 20 mai. 2013.

125 SHOSTAK, 2013.

126 MENGER, 1892, p. 241. Na terminologia atual, “vendabilidade” seria mais bem definida como liquidez. O sentido pretendido pelo autor é precisamente o de diferentes graus de liquidez que diferentes bens apresentam.

127 MISES, 1953, p. 33.

128 Ibid.

129 Usando a cotação registrada ao fim de 2013, 1.202 dólares por onça Troy de ouro, um grama equivale a 38 dólares. Em termos físicos, um grama de ouro é menor do que uma unha humana. Seria inviável fazer compras do cotidiano com, por exemplo, um decigrama de ouro (3,8 dólares).

130 ROTHBARD, Murray N. Man, Economy and State with Power and Market. Auburn: Ludwig von Mises Institute, 2004. p. 192-193.

131 Não tenho dúvidas de que Rothbard concordaria com essa lógica, tendo ele apenas simplificado a definição de moeda para os propósitos de explicação das trocas indiretas. Contudo, escolhemos o trecho para contrastar a ideia de que qualquer bem usado como meio de troca jamais poderia ser taxado efetivamente de moeda.

132 Outro exemplo, este real, que também ilustra a imprecisão que seria qualificar qualquer meio de troca de moeda, é o caso do blogueiro canadense Kyle MacDonald. De julho de 2005 a julho de 2006, Kyle ficou famoso por trocar um simples clipe vermelho por diversos outros bens, em um total de 14 transações consecutivas, até atingir seu objetivo final, a aquisição de uma casa. Certamente não poderíamos considerar como moeda cada bem aceito por Kyle em cada uma das 14 transações. Disponível em: <http://en.wikipedia.org/wiki/One_red_paperclip>. Acesso em: 28 dez. 2013.

133 *Currency* advém do latim, da palavra *currens*, particípio presente do verbo *currō*, que significa correr. *Currens*, em português, equivale a “corrente”, aquilo que corre ou está em curso.

134 Para um breve resumo do colapso monetário do Ocidente, ver ROTHBARD, 2013.

135 HICKS, John R., A Suggestion for Simplifying the Theory of Money, Economica, February 1935, p. 1-19 apud HAYEK, F. A. Desestatização do Dinheiro. São Paulo: Instituto Ludwig von Mises Brasil, 2011. p. 66.
136 HAYEK, 2011. p. 66.
137 Ibid., p. 67.
138 Em *Theory of Money and Credit*, ao contemplar qual a moeda única que prevalecerá mundialmente, Mises afirma que "Não será possível pronunciar o veredito final até que todas as principais partes habitadas da Terra formem uma única área comercial, porque enquanto isso não acontecer, será impossível que outras nações com sistemas monetários adiram à área comum e modifiquem a organização internacional", MISES, 1953, p. 33. Essa declaração nos faz imaginar: e quando o comércio do homem no universo ultrapassar os limites do planeta Terra? Nesse cenário, qualificar um bem como moeda seria, assim, uma tarefa quase impossível.
139 Triennial Central Bank Survey of foreign exchange and derivatives market activity in 2013. Disponível em: <http://www.bis.org/publ/rpfx13fx.pdf>. Acesso em: 10 jan. 2014.
140 Outros ativos podem servir como reserva de valor (ex.: imóveis), mas a liquidez destes pode ser bastante reduzida, sendo preciso, na maior parte das vezes, trocá-los por moedas (ou "monetizá-los") quando a sua utilização for necessária.
141 Bitcoin poderia ser considerado, dependendo do momento, uma moeda secundária, pois há casos em que ela acaba sendo convertida em moedas nacionais para concluir uma transação.
142 MISES, 1953, p. 34,
143 MISES, 2010, p. 465.
144 MISES, 2010, p. 276.
145 MENGER, 1892, p. 245.
146 HÜLSMANN, Jörg Guido. The Ethics of Money Production. Auburn: Ludwig von Mises Institute, 2008.

A liberdade monetária e o Bitcoin

"A moeda não foi gerada pela lei. Na sua origem, ela é uma instituição social, não estatal."

Carl Menger, *On the origins of money*

"Dinheiro é um fenômeno do mercado. O que isso significa? Significa que o dinheiro desenvolveu-se no mercado, e seu desenvolvimento e funcionamento não têm nada a ver com o governo, o estado ou a violência exercida pelos governos."

Ludwig von Mises, *On money & inflation*

"Não poderia haver um freio melhor contra o abuso da moeda pelo governo do que se as pessoas fossem livres para recusar qualquer moeda que desconfiassem e preferir uma moeda na qual confiam... Parece-me que se conseguíssemos impedir governos de se intrometer com a moeda, faríamos um bem maior do que qualquer governo já fez a esse respeito."

F.A. Hayek, *Choice in currency*

DESDE TEMPOS IMEMORIAIS, é vedada aos indivíduos a liberdade de escolha de moeda. Somos obrigados a usar um dinheiro estatal, constantemente abusado e depreciado. Não obstante, moeda honesta e sadia é uma precondição básica para uma sociedade próspera e livre. Mas alcançar esse ideal pela via política é algo bastante intricado.

Nesta última seção, faz-se necessário entender o valor de uma moeda livre para a prosperidade e liberdade de cada indivíduo e da sociedade como um todo. E, uma vez compreendida a noção de dinheiro livre, recordaremos sucintamente algumas das diversas tentativas e propostas de reformas do sistema monetário ao longo da história, identificando as principais causas dos seguidos malogros.

Diante de todo o conhecimento aqui organizado e elaborado, será possível, então, não somente perceber como o Bitcoin se encaixa nesse estado de coisas, mas também captar a essência do fenômeno, a sua força motriz. Por fim, e concluindo a obra, nos lançaremos à arriscada missão de conjecturar e prever o futuro da moeda digital.

1. A importância da liberdade monetária para uma sociedade próspera e livre

O senso comum costuma atribuir ao dinheiro a causa de todos os males. Em realidade, sem o dinheiro, a sociedade como hoje existe seria inconcebível. Dinheiro é um meio de troca, é o grande facilitador dos intercâmbios realizados no mercado. É ele que permite a divisão do trabalho, possibilitando que cada produtor se especialize naquilo que melhor produz. O aprofundamento da divisão do trabalho aumenta a produtividade da economia e a capacidade de poupança, que, por sua vez, viabilizam o investimento e o acúmulo de capital. A constante multiplicação do capital acumulado significa que a economia cresce e prospera e que, assim, a sociedade cria riqueza e é capaz de melhorar o padrão de vida dos seus cidadãos.

Dinheiro não é um mal; é, na verdade, o bem fundamental em qualquer economia minimamente complexa. Tivéssemos que voltar ao escambo, nossa economia não seria capaz de alimentar mais do que um punhado de famílias. Em definitivo, o dinheiro é uma das instituições mais essenciais de uma civilização; é o bem que torna possível a cooperação social em larga escala.

Dessa forma, toda agressão contra a moeda gerará consequências gravíssimas no funcionamento da economia. A falsificação e a depreciação da unidade monetária, historicamente um privilégio de soberanos e governos, geram efeitos perniciosos na sociedade, impedindo uma cooperação social tranquila. A intervenção estatal na moeda como hoje a conhecemos não é diferente. O monopólio de emissão de moeda e o sistema bancário cartelizado pelo próprio governo são responsáveis por grande parte dos problemas econômicos enfrentados pela sociedade moderna.

Quando analisamos a história da moeda, encontramos um registro sucessivo de episódios recorrentes de agressão ao dinheiro da sociedade. Das técnicas indecentes de envilecimento das moedas à moderna e ilimitada criação de moeda fiduciária eletrônica, quem paga a conta pela inflação é sempre a sociedade, em especial, os mais pobres. O imposto inflacionário, a forma mais indigna e abominável de expropriar riqueza dos indivíduos, não é nem sequer compreendido por grande parte da sociedade. Como o próprio Keynes expressou ao constatar que Lenin tinha razão sobre a inflação como forma de subverter o sistema capitalista:

> Não há maneira mais sútil nem mais segura de derrubar a base da sociedade do que perverter a moeda. O processo engrena todas as forças ocultas da lei econômica no lado da destruição e o faz de tal forma que nem um homem dentre um milhão é capaz de diagnosticar.[147]

A inflação é o artifício mais eficiente para financiar os gastos do estado sem precisar recorrer ao impopular e visível imposto. E é, simultaneamente, uma forma de redistribuição de riqueza, pois qualquer inflação, qualquer aumento na quantidade de dinheiro na economia, não é neutra. Há ganhadores e perdedores, nem sempre perfeitamente identificados. Enriquecem aqueles que primeiro recebem a moeda recém-criada, porque são capazes de adquirir bens e serviços aos preços ainda correntes. Estes são os recipientes mais próximos do dinheiro novo, como políticos, servidores públicos e as empresas dos setores ora beneficiados pelo gasto público. Empobrecem aqueles que por último recebem a moeda de nova criação, porque, após ela circular pela economia, o aumento da oferta monetária conduzirá necessariamente a uma diminuição no seu poder de compra, ou, o seu corolário, a uma elevação generalizada dos preços. Quem são esses perdedores? Quem depende de um salário fixo ao fim de cada mês. Normalmente, os mais pobres da sociedade, que, quando do recebimento de seus proventos, não mais poderão obter o que o seu dinheiro antes comprava. A inflação é a causa principal da desigualdade em um país. E quanto maior sua intensidade, piores suas consequências.

Não há dúvidas de que grande parte da desigualdade social brasileira reside justamente na emissão descontrolada de moeda nas décadas passadas – quase sempre sob os mantos intocáveis da industrialização, das políticas sociais e do assistencialismo. Moeda sadia não faz parte da cultura e história luso-brasileira[148]. No Brasil, a perversão da moeda é norma histórica e princípio nuclear da política social. É verdade que o Plano Real nos propiciou um mínimo de civilidade monetária, mas, ainda assim, em grau aquém do desejável quando comparado ao de países desenvolvidos.

O caso brasileiro, singular e com poucos paralelos pelo mundo, é o que Mises denominava de

inflação simples, em que a emissão de moeda ocorre essencialmente com o propósito de financiamento direto do estado; a gestão monetária é nitidamente uma atividade política. Nesse arranjo, o aumento da oferta monetária gera principalmente uma diminuição do poder aquisitivo da moeda, com efeitos secundários na atividade econômica.

Entretanto, a inflação hoje em dia é gerada de forma mais complexa e envolve bancos centrais e todo o sistema bancário. E embora ela também sirva como fonte de custeio fiscal, essa função é indireta e um tanto imperceptível[149]. Bancos centrais relativamente independentes – embora existam somente com o amparo legal e a maior parte de seus incumbentes seja indicada politicamente – controlam a oferta de moeda de forma monopolística, regulando e supervisionando todo o sistema bancário. Essa é a ordem que vigora em quase todos os países modernos. A consequência não intencionada são os recorrentes ciclos econômicos, episódios de auge e recessão em que a atividade econômica é artificialmente fomentada, gerando uma falsa prosperidade que contém as sementes de sua própria destruição. O caso mais recente, a crise de 2008, é um perfeito exemplo da ingerência estatal da moeda conforme estruturada no presente. Embora possamos considerar essa ordem monetária superior à simples emissão de moeda pelo estado em seu próprio e direto benefício, ela é igualmente instável e insustentável. Existe e perdura por força de lei, não pela escolha do mercado. A doutrina da moeda estatal não admite concorrência.

A ordem monetária vigorante é uma criatura disforme, filha das urgências fiscais de governos, como a suspensão da conversibilidade das moedas nacionais em ouro para financiar a Primeira Guerra Mundial - encerrando assim um longo ciclo de estabilidade monetária. Apuros fiscais e má gestão da moeda conduziram inevitavelmente à abolição do padrão-ouro. É preciso frisar, no entanto, que o metal precioso não colapsou, nem mesmo falhou como padrão monetário. O fracasso, de fato, deveu-se aos estados, descontentes com a disciplina imposta pelo padrão-ouro, pois este era o último empecilho à livre emissão de moeda, seja para financiar guerras, seja para bancar o estado de Bem-Estar Social. O que temos hoje é um sistema monetário elástico, cuja emissão de moeda é uma mera função da vontade política embasada por teorias econômicas defeituosas[150].

O peso dos estados modernos na economia é uma realidade preocupante, e sua sobrevida é facilitada pelo controle monopolístico da moeda. E todo aumento de poder, toda expansão do estado, redunda em perda de liberdade. Moeda honesta é, sobretudo, um limitador ao crescimento do estado. É uma forma de impor disciplina a um ente indisciplinado por natureza.

Contudo, os efeitos de uma moeda estatal não têm reflexos somente no crescimento do poder do estado. A inflação molda o comportamento dos indivíduos, provocando distúrbios na cooperação social, deixando marcas na cultura e na conduta humana em sociedade que seguem presentes por gerações. Governo hipercentralizado, ciclos de auge e recessão, o jugo da dívida – a poupança é suplantada pelo crédito como motor de crescimento –, a especulação financeira desenfreada, a desconfiança entre consumidores e produtores, etc., são alguns traços do legado cultural e espiritual da inflação monetária[151].

Moeda honesta é, portanto, o ideal ao qual todo defensor da liberdade deveria aspirar. A raiz de todos os males não é o dinheiro; é, na verdade, a inflação, cuja semente germina no controle estatal da moeda. Liberdade monetária significa liberdade de escolha de moeda; significa também liberdade de produção de moeda em um ambiente de livre concorrência. Como Hayek postulou há quase 40 anos em defesa da livre produção de moedas privadas, “Um bom dinheiro só pode surgir do interesse próprio, e não da benevolência. Sempre tivemos moeda ruim porque

a empresa privada não teve permissão de nos fornecer uma melhor”[152].

2. As propostas de reformas pelos liberais

Desde a tradição iniciada por Ludwig von Mises, todo economista da Escola Austríaca de economia buscou estudar como reformar o sistema monetário vigente. O princípio de moeda sadia guiou as doutrinas e políticas monetárias do século XIX, mas somente no século passado foi ele estendido, englobando os preceitos não somente de uma moeda sólida, mas também – e sobretudo – de uma moeda livre da ingerência estatal.

Dentre os principais expoentes de propostas à reconstrução monetária estão os economistas liberais Ludwig von Mises, Murray N. Rothbard, F. A. Hayek, Hans Sennholz, Jesús Huerta de Soto e Philipp Bagus. Entretanto, e como a realidade inexorável atesta, nenhuma proposta teve sucesso. Ou, mais bem dito, nenhuma foi sequer implantada.

Embora todas defendam o princípio de moeda sólida como fim, as propostas pecam nos meios para atingir esse ideal. Igualmente, cada uma tem suas vantagens e desvantagens, pontos meritórios, medidas intervencionistas, arbitrariedades, etc.[153] Mas todas convergem ao mesmo problema central: para serem implantadas, dependem da decisão política. Estão subordinadas à promulgação e aplicação de leis. Nem mesmo a ideia de reforma mais radical, a de *Button-Pushing* de Philipp Bagus[154], escapa desse ponto nevrálgico. Em suma, são todas politicamente inviáveis.

Isso não significa que sejam politicamente impossíveis, meramente que, neste instante do tempo, alcançar esse objetivo pela via política é altamente improvável. E por que é altamente improvável? Primeiro, porque uma reforma monetária e bancária liberal afronta quem mais se beneficia do status quo, o governo e os bancos. Um governo legislará contra seu próprio interesse somente no instante em que a causa for pauta política capaz de decidir eleições. E como pode o ideal de liberdade monetária ser um tema comum e discutido pela sociedade a ponto de tornar-se uma questão política? Como convencer a maioria da população acerca da necessidade e dos benefícios de tal medida? Não há atalhos, a única via passa pela educação. “Há, portanto, uma imensa tarefa educacional à nossa frente antes que possamos ter a esperança de nos libertarmos da mais grave ameaça à paz social e à contínua prosperidade, inerente às instituições monetárias atuais”, concluiu Hayek[155]. Definitivamente, concordamos com essa afirmação, é preciso educar a sociedade.

Mas sejamos realistas: quando podemos esperar a materialização dessa tarefa? A compreensão dos fenômenos monetários não é algo simples, não é algo que o cidadão médio seja capaz de absorver facilmente. O ideal de liberdade monetária, portanto, a ser atingido pela via política está condicionado à educação de grande parte da sociedade, de modo a tornar a questão não só relevante, mas também crítica no processo democrático. Seria razoável esperar que isso se torne realidade? Infelizmente, considero bastante improvável persuadir a opinião pública na direção de uma moeda livre assegurada por força de lei. Porque, além de conseguir a adoção de políticas públicas com esse viés, a manutenção da reforma, a sua sustentabilidade, dependerá também de uma sociedade educada na matéria, ou testemunharemos os avanços obtidos ruírem na demagogia do próximo governante populista.

Precisamente neste ponto jaz uma das forças do Bitcoin. Ao invés de implorar pelo respaldo

legal, ele o contorna. Ao invés de pedir permissão para operar, ele simplesmente existe. O Bitcoin não é uma criatura do estado, é uma invenção e evolução do mercado que independe do consentimento do poder público. É claro que as decisões políticas podem influenciar a conduta dos indivíduos e das empresas, mas aquelas, por si só, são incapazes de coibir o livre funcionamento da moeda digital. Anular o poder proibidor dos governos é algo inédito na história da humanidade.

3. Bitcoin contra a tirania monetária

A moeda digital criada por Satoshi Nakamoto proporciona enormes vantagens comparativas em relação às demais moedas fiduciárias. Mas Bitcoin não é apenas uma forma de realizar transações globais com baixo ou nenhum custo. Bitcoin é, em realidade, uma forma de impedir a tirania monetária. Essa é a sua verdadeira razão de ser[156].

O entorno do surgimento da moeda digital não foi nenhuma coincidência. Bitcoin emergiu como uma resposta natural ao colapso da atual ordem monetária, à constante redução de privacidade financeira e a uma arquitetura bancária cada vez mais prejudicial ao cidadão comum. Governos não podem inflacionar bitcoins. Governos não podem apropriar-se da rede Bitcoin. Governos tampouco podem corromper ou desvalorizar bitcoins. E também não podem proibir-nos de enviar bitcoins a um comerciante no Maranhão ou no Tibete.

Imaginem um mundo sem inflação, sem bancos centrais desvalorizando o seu dinheiro para financiar a esbórnia fiscal dos governantes. Sem confisco de poupança. Sem manipulação da taxa de juros. Sem controle de capitais. Sem banqueiros centrais deificados e capazes de dobrar a base monetária a esmo e a qualquer instante para salvar banqueiros ineptos que se apropriaram dos seus depósitos em aventuras privadas. A verdade é que o Bitcoin, ou o que vier a substituí-lo no futuro, impõe uma verdadeira concorrência contra o cartel dos banqueiros e a moeda dos governos. Por isso, não esperemos nenhuma boa vontade dessa dupla simbiótica em relação ao Bitcoin.

A internet nos permitiu a liberdade de comunicação. O Bitcoin tem o potencial de devolver nossa liberdade sobre nossas próprias finanças. Bitcoin é a internet aplicada ao dinheiro.

Como o próprio Satoshi Nakamoto expressou em certa ocasião:

> O problema básico com a moeda convencional é toda a confiança necessária para fazê-la funcionar. Precisamos confiar que o banco central não desvalorizará o dinheiro, mas a história das moedas fiduciárias está repleta de quebras dessa confiança. Bancos têm a obrigação de guardar nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito com uma mera fração em reserva. Temos que confiar-lhes com nossa privacidade, confiar que não deixarão ladrões de identidade drenar nossas contas.[157]

O Bitcoin dispensa a dependência de intermediários fiduciários que historicamente violaram os direitos de seus clientes. Ele impede a tirania monetária, tornando-a praticamente impossível. Para qualquer defensor da liberdade, é um feito louvável; para cidadãos de regimes autoritários, é uma necessidade imprescindível. Em definitivo, qualquer nação com histórico recorrente de agressões contra a moeda será muito beneficiada pelo uso do Bitcoin. Os brasileiros, por exemplo, tão calejados por diversos planos econômicos malfadados, têm muito a ganhar com

uma moeda que os protege genuinamente das arbitrariedades de governos que, ao longo da história, abusaram do poder, infringindo impiedosamente os direitos de propriedade de seus cidadãos.

A história da humanidade é um atestado de uma triste verdade: nenhum sistema político foi capaz de conter os abusos de governos no âmbito monetário. Bitcoin nasce, assim, como uma alternativa necessária, porque quando as Constituições e a separação dos poderes são incapazes de assegurar uma moeda inviolável, a tecnologia se encarrega de fazê-lo. A separação do estado e da moeda será uma questão tecnológica, não política.

4. O futuro do Bitcoin

Embora possa parecer que haja uma dicotomia entre o Bitcoin e as moedas fiduciárias, em realidade, é preciso enxergar o Bitcoin não como mutuamente excludente, mas sim como complementário às formas de dinheiro até hoje existentes. É verdade que não podemos saber se o Bitcoin irá perdurar. Não sabemos se sobreviverá outro ano, ou uma década. Mas arrisco dizer que uma moeda digital (ou criptomoeda) veio para ficar. “O preço do Bitcoin pode até colapsar, e os usuários podem repentinamente migrar para outra moeda”, escreveu a revista Britânica *The Economist* em artigo sobre o Bitcoin, “mas há grande probabilidade de que alguma forma de dinheiro digital deixará uma marca duradoura no ambiente financeiro”[158].

Há inúmeras vantagens que fazem de uma moeda digital um excelente complemento no meio financeiro. No seu atual estágio, o Bitcoin já representa uma substancial redução nos custos de transação. Portanto, independentemente da sua liquidez futura, ele já atua como um meio de troca, já é uma moeda, embora menos líquida do que as moedas nacionais. Dessa forma, poderíamos até considerá-lo o precursor de uma nova classe de ativos: a das “moedas digitais”.

Apesar de ser uma tecnologia inovadora com potencial de trazer inúmeros benefícios à sociedade, ainda há importantes barreiras a serem ultrapassadas. Especialmente no âmbito legal e regulatório, ainda há enormes incertezas quanto à ação dos governos diante do crescimento do Bitcoin. Muitos adeptos da moeda digital clamam pela legitimidade legal, sob a justificativa de que ela é necessária para o seu desenvolvimento. É verdade que logo as autoridades terão de se pronunciar, pois a ampliação do uso do Bitcoin obrigará os governos a esclarecerem de que forma as transações com a moeda serão tributadas. Contudo, não devemos esperar aplausos de algum órgão regulador, nem apoio ou qualquer atitude efusiva oriunda do setor público em relação às moedas digitais. Afinal de contas, como guardiões da moeda e da estabilidade financeira, bancos centrais e reguladores têm por ofício a incumbência de gritar fogo ao menor sinal de perigo. Além disso, no momento em que o Bitcoin for percebido como um concorrente genuíno à moeda estatal e ao sistema bancário, o tratamento legal dado a ele poderá ser bastante negativo.

Embora a necessidade de legitimidade legal possa ser questionada, não há dúvidas de que a legitimidade de mercado é fundamental ao avanço e desenvolvimento do Bitcoin. Como os indivíduos, as empresas e o comércio em geral percebem a moeda é e será fator decisivo no progresso e na ampliação de seu uso. Por essa razão, é notável o fato de grandes empresas passarem a aceitar o Bitcoin[159] por questões mercadológicas, e não apenas como uma mera tática de marketing. O ano de 2014 será, possivelmente, repleto de notícias de novas empresas, novos comerciantes e afins adotando o Bitcoin como uma nova forma de pagamento. Arrisco

dizer que o preço ficará em segundo plano. O tema central será a convergência do mercado à mais nova tecnologia financeira dos últimos anos. A adesão ao Bitcoin está prestes a tornar-se um imperativo de mercado. Essa, sim, é a legitimidade essencial ao futuro da moeda digital.

Mas, sem dúvida alguma, essa nova moeda enfrentará obstáculos ao longo do percurso. Haverá volatilidade, possíveis bolhas e quedas, casas de câmbio serão fechadas, outras quebrarão, e novas formas de usar a moeda surgirão. O livre mercado certamente saberá contornar os percalços e progredir. A inata capacidade criativa do ser humano é o motor do progresso, e nela reside meu otimismo em relação ao futuro do Bitcoin.

Como tecnologia, aos poucos o protocolo Bitcoin vai sendo descoberto pelo que realmente é: uma forma revolucionária de criar, transitar e estocar informação prescindindo de qualquer intermediário; uma forma inovadora para transferência de propriedade. A moeda foi apenas a primeira aplicação; no futuro, é provável que a tecnologia seja aproveitada em várias outras indústrias.

Por fim, e voltando ao Bitcoin como uma nova forma de dinheiro, deixo uma sugestão aos economistas: estudem a moeda digital a fundo. Não a desmereçam pela simples aparência virtual. De fato, o Bitcoin tem forçado os estudiosos da teoria monetária e bancária a revisitar conceitos que pareciam estar completamente compreendidos e superados. Temos uma oportunidade ímpar de refinar a teoria acerca dos fenômenos monetários. Àqueles que prezam a liberdade, reitero que, pela primeira vez na história da humanidade, a possibilidade de não dependermos de nenhum órgão central controlando nosso dinheiro é real e está se desenrolando neste exato instante diante de nossos olhos. É a primeira moeda verdadeiramente global desde que o ouro foi forçadamente desmonetizado. À liberdade individual e ao desenvolvimento da civilização, as consequências desse arranjo são extraordinárias e sem precedentes. Dinheiro honesto é uma questão sobretudo moral e basilar para qualquer sociedade que almeja a paz e a prosperidade. E é precisamente essa a essência do experimento Bitcoin.

Mas não esperemos, como sinal de sucesso, que a moeda digital venha algum dia a suplantar as moedas estatais. Basta o Bitcoin servir ao menos como um firme e confiável empecilho ao abuso irrestrito do nosso dinheiro pelos governos, e ele já terá seu nome gravado na história da liberdade.

Em 2008, Satoshi Nakamoto supostamente teria dito que o Bitcoin “é muito atrativo do ponto de vista libertário, se conseguirmos explicá-lo adequadamente. Mas infelizmente sou melhor com código de programação do que com palavras”.

Espero que esta obra tenha ajudado a explicar um pouco melhor em palavras o significado revolucionário dos códigos do Bitcoin.

Rodapé

147 KEYNES, John Maynard. As Consequências Econômicas da Paz. Brasília: UnB, 2002.
148 MEIRA PENNA, J.O. de. Em berço esplêndido – ensaios de psicologia coletiva brasileira. Rio de Janeiro: Topbooks, 1999.
149 Quando o governo precisa de recursos, além dos impostos arrecadados, ele emite títulos de dívida, que, por sua vez, são adquiridos pelos bancos chamados de *dealers primários* pela simples criação de moeda bancária (ou escritural) do nada. Por outro lado, o banco central realiza sua política monetária comprando e vendendo títulos públicos desses mesmos bancos – igualmente, criando moeda do nada –, criando assim um mercado cativo e assegurando liquidez suficiente aos títulos de dívida emitidos pelo estado.
150 SCHLICHTER, Detlev. Paper Money Collapse – the folly of elastic money and the coming monetary breakdown.

New Jersey: John Wiley & Sons, 2011.
151 HÜLSMANN, 2008.
152 HAYEK, 2011, p.154.
153 Recomendo fortemente a análise crítica feita por Philipp Bagus em *Monetary Reform and Deflation – A Critique of Mises, Rothbard Huerta de Soto and Sennholz*, New Perspectives on Political Economy, Volume 4, Number 2, 2008, pp. 131-157.
154 Bagus defende, bascimaente, a remoção imediata e simultânea de todas as intervenções e privilégios nos âmbitos monetário e bancário. BAGUS, Philipp, *Monetary Reform– The Case for Button-Pushing*, New Perspectives on Political Economy, Volume 5, Number 2, 2009, pp. 111-128.
155 HAYEK, 2011, p. 156.
156 MATONIS, Jon. Bitcoin Prevents Monetary Tyranny, Forbes, 4 abr. 2012. Disponível em: <http://www.forbes.com/sites/jonmatonis/2012/10/04/bitcoin-prevents-monetary-tyranny/>. Acesso em: 15 mai. 2013.
157 Disponível em: <http://p2pfoundation.net/Bitcoin>. Acesso em: 10 jan. 2014.
158 Mining digital gold. The Economist, 13 apr. 2013. Disponível em: <http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital>. Acesso em: 20 mai. 2013.
159 ULRICH, Fernando. Uma semana histórica para o Bitcoin. InfoMoney, 13 jan. 2014. Disponível em: <http://www.infomoney.com.br/blogs/moeda-na-era-digital/post/3143266/uma-semana-historica-para-bitcoin>. Acesso em: 13 jan. 2013.

Dez formas de explicar o que é o Bitcoin

Para aqueles que desejam uma rápida fonte de referência para explicar o que é o Bitcoin, este breve texto será de muita utilidade. Porque, à primeira vista, entender o que é Bitcoin não é uma tarefa fácil. A tecnologia é tão inovadora, abarca tantos conceitos de distintos campos do conhecimento humano – e, além disso, rompe inúmeros paradigmas – que explicar o fenômeno pode ser uma missão ingrata.

Acredito que iniciar qualquer explicação com “criptografia”, “rede *peer-to-peer*”, “chave pública”, “mineração em computador”, “consenso distribuído”, etc. é, em geral, um péssimo começo. Mas depende muito do seu interlocutor, é claro.

Explicar o que é Bitcoin é um processo gradual e progressivo. Você não começa detalhando todas as nuances do protocolo e como a criptografia moderna é empregada em uma rede de computadores totalmente distribuída. Não. Você deve iniciar do básico. E, preferencialmente, deve procurar explicá-lo relacionando-o com a realidade de cada pessoa.

Curiosamente, o Bitcoin reúne duas instituições que poucos sabem descrever e interpretar, mas muitos as usam diariamente: o dinheiro e a internet. É como o Nassim Taleb afirma em seu livro Antifragile: “O conhecimento não exclui o uso”.

Dito isso, e sendo o Bitcoin uma tecnologia nascente e inovadora, muitos querem entendê-lo, para poder usá-lo. Absolutamente compreensível. Assim, não nos esquivaremos da missão de desvendá-lo. O que se segue são meras sugestões para iniciar a explicação do Bitcoin, pois além deste passo introdutório acabaríamos enredados em detalhes desimportantes para muitos (neste caso, melhor ler todo o livro de uma vez). Considerando os possíveis e distintos interlocutores, elenquei abaixo alguns importantes, aos quais recomendo as seguintes explicações quando você apresentar o Bitcoin:

Ao cidadão comum: Bitcoin é uma forma de dinheiro, assim como o real, dólar ou euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações online, é a forma ideal de pagamento, pois é rápido, barato e seguro. É uma tecnologia inovadora.

À geração Y: Você lembra como a internet e o e-mail revolucionaram a comunicação? Antes, para enviar uma mensagem a uma pessoa do outro lado da Terra, era necessário fazer isso pelos correios. Nada mais antiquado. Você dependia de um intermediário para, fisicamente, entregar uma mensagem. Pois é, retornar a essa realidade é inimaginável. O que o e-mail fez com a informação, o Bitcoin fará com o dinheiro. Com o Bitcoin você pode transferir fundos de A para B em qualquer parte do mundo sem jamais precisar confiar em um terceiro para essa simples tarefa.

Ao banqueiro: Bitcoin é uma moeda e um sistema de pagamento em que o usuário, dono da moeda, custodia o seu próprio saldo. Isso quer dizer que o usuário é seu próprio banco, pois ele é depositante e depositário ao mesmo tempo. Nesse sistema, os usuários podem efetuar transações entre si sem depender de um intermediário ou casa de liquidação, independentemente da localização geográfica de cada um. Similarmente à moeda escritural, de criação exclusiva do sistema bancário, o bitcoin é uma moeda incorpórea.

Ao banqueiro suíço: Bitcoin é como uma conta bancária suíça numerada que pode existir no seu próprio smartphone. Com ele, é possível fazer transações online com quase nenhum custo. É como se você tivesse um supercartão de débito bancário, ainda que não haja nenhum cartão físico e nem mesmo um banco por trás. E somente bitcoins podem circular nesse sistema.

Ao banqueiro central: Bitcoin é uma moeda emitida de forma descentralizada seguindo as regras de uma política monetária não discricionária e altamente rígida. O objetivo principal da política monetária do Bitcoin é o crescimento da oferta de moeda, o qual é predeterminado e de conhecimento público. Além disso, o Bitcoin é, ao mesmo tempo, uma unidade monetária e um sistema de pagamentos e de liquidação. Dessa forma, os usuários transacionam entre si e diretamente, sem depender de um terceiro fiduciário.

Ao contador: Bitcoin é como um grande livro-razão, único e compartilhado por todos os usuários simultaneamente. Nele, todas as transações são registradas, sendo verificadas e validadas por usuários especializados, de modo a evitar o gasto duplo e que usuários gastem saldos que não possuem ou de terceiros. Esse registro público universal e único não pode ser forjado. Lá estão devidamente protocoladas todas as transações já realizadas na história do Bitcoin, bem como os saldos atualizados de cada usuário. O livro-razão é, assim, um registro fidedigno, estando sempre atualizado e conciliado. Por sinal, o nome dado a esse livro-razão é *blockchain*.

Ao economista: Bitcoin é uma moeda, um meio de troca, embora ainda pouco líquida quando comparada às demais moedas existentes no mundo. Em algumas regiões de opressão monetária, é cada vez mais usada como reserva de valor. Uma característica peculiar é a sua oferta limitada em 21 milhões de unidades, a qual crescerá paulatinamente a uma taxa decrescente até alcançar esse limite máximo. Embora intangível, o protocolo do Bitcoin garante, assim, uma escassez autêntica. Como unidade de conta, pode-se afirmar que ainda não é empregada como tal, devido, especialmente, à sua volatilidade recente. Ademais, Bitcoin é também um sistema de pagamentos, o que significa que, pela primeira vez na história da humanidade, a unidade monetária está aliada ao sistema bancário e de pagamento e é parte intrínseca dele.

Ao jurista: bitcoins, como unidade monetária, são mais bem considerados um bem incorpóreo que, em certos mercados, têm sido aceitos em troca de bens e serviços. Poderíamos dizer que essas transações constituem uma permuta, e jamais venda com pagamento em dinheiro, pois a moeda, em cada jurisdição, é definida por força de lei, sendo uma prerrogativa de exclusividade do estado.

Ao pessoal de TI: Bitcoin é um software de código-fonte aberto, sustentado por uma rede de computadores distribuída (*peer-to-peer*) em que cada nó é simultaneamente cliente e servidor. Não há um servidor central nem qualquer entidade controlando a rede. O protocolo do Bitcoin, baseado em criptografia avançada, define as regras de funcionamento do sistema, às quais todos os nós da rede aquiescem, assegurando um consenso generalizado acerca da veracidade das transações realizadas e evitando qualquer violação do protocolo.

Ao cientista físico: Bitcoin é um software que, portanto, inexiste materialmente. Uma unidade monetária de bitcoin nada mais é do que um apontamento contábil eletrônico, no qual são registrados a conta-corrente (o endereço do Bitcoin ou a chave pública) e o saldo de bitcoins em dado momento. Nesse sentido, uma unidade de bitcoin não difere em nada de uma unidade de real ou dólar depositada em um banco, pois é igualmente um mero registro contábil eletrônico. Mas há uma grande diferença; no caso do Bitcoin, o espaço no qual os registros são efetuados é único, universal e compartilhado por todos os usuários (o *blockchain*), enquanto no sistema atual, cada banco detém e controla o seu registro de transações (o seu próprio livro-razão).

Longe de serem exaustivas, essas breves explicações servem para elucidar um pouco e de forma rápida o significado do fenômeno.

O que o Bitcoin representa pode variar de acordo com a ocupação e a realidade de cada pessoa. Mas, sem dúvida alguma, é uma tecnologia revolucionária, e isso independe de qualquer interpretação pessoal.

Referências

ANDREESSEN, Marc. **Why Bitcoin Matters**. 22 jan. 2014. Disponível em: <http://blog.pmarca.com/2014/01/22/why-bitcoin-matters/>. Acesso em: 26 jan. 2014.

BAGUS, Philipp. **Monetary Reform and Deflation** – A Critique of Mises, Rothbard Huerta de Soto and Sennholz. New Perspectives on Political Economy, Volume 4, Number 2, 2008. pp. 131-157.

______. **Monetary Reform** – The Case for Button-Pushing. New Perspectives on Political Economy, Volume 5, Number 2, 2009. pp. 111-128.

BERNANKE, Ben. Monetary Policy since the Onset of the Crisis. **Federal Reserve**, 31 ago. 2012. Disponível em: < http://www.federalreserve.gov/newsevents/speech/bernanke20120831a.htm>. Acesso em: 27 dez. 2013.

BÖHM-BAWERK, Eugen. **Whether Legal Rights And Relationships Are Economic Goods**. Shorter Classics Of Eugen Von Böhm-Bawerk Volume I, South Holland: Libertarian Press, 1962.

BRITO e CASTILLO. **Bitcoin**: A Primer for Policymakers. Arlington: Mercatus Center at George Mason University, 2013.

BRITO, Jerry. **The Top 3 Things I Learned at the Bitcoin Conference**. Reason, 20 mai. 2013. Disponível em: <http://reason.com/archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoi>. Acesso em: 12 dez. 2013.

______. National Review Gets Bitcoin Very Wrong. **Technology Liberation Front**, 20 jun. 2013. Disponível em: <http://techliberation.com/2013/06/20/national-review-gets-bitcoin-very-wrong/>. Acesso em: 14 dez. 2013.

BUTERIN, Vitalik. Bitcoin Store Opens: **All Your Electronics Cheaper with Bitcoins**. Bitcoin Magazine, 5 nov. 2012. Disponível em: <http://bitcoinmagazine.com/bitcoin-store-opens-all-your-electronics-cheaper-with-bitcoins/>. Acesso em: 10 dez. 2013.

CHRISTIN, Nicolas. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. **Carnegie Mellon CyLab Technical Reports**: CMU-CyLab-12-018, 30 jul. 2012 (atualizado em 28 Nov. 2012). Disponível em: <http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf>. Acesso em: 14 dez. 2013.

COLDEWEY, Devin. $250,000 **Worth of Bitcoins Stolen in Net Heist**. NBC News, 5 set. 2012. Disponível em: <http://www.nbcnews.com/technology/250-000-worth-bitcoins-stolen-net-heist-980871>. Acesso em: 14 dez.2013.

DAI, Wei. **Bmoney**. Disponível em: <http://www.weidai.com/bmoney.txt>. Acesso em: 21 dez. 2013.

DUNCAN, Andy. The Great Gold vs. Bitcoin Debate: Casey vs. Matonis. **Lew Rockwell**, 15

abr. 2013. Disponível em: <http://lewrockwell.com/orig11/duncan-a4.1.1.html>. Acesso em: 20 mai. 2013.

FARRELL, Maureen. **Strategist Predicts End of Bitcoin**. CNNMoney, 14 mai.2013. Disponível em: <http://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/index.html>. Acesso em: 13 dez. 2013.

FONG, Jeff. **How Bitcoin Could Help the World's Poorest People**. PolicyMic, mai. 2013. Disponível em: <http://www.policymic.com/articles/41561/bitcoin-price-2013-how-bitcoin-could-help-the-world-s-poorest-people>. Acesso em: 12 dez. 2013.

GERTCHEV, Nikolay. **The Money-ness of Bitcoins**. Mises Daily, Auburn: Ludwig von Mises Institute, 4 abr. 2013. Disponível em: <http://mises.org/daily/6399/The-Moneyness-of-Bitcoins>. Acesso em: 22 dez. 2013.

GRAF, Konrad S. **Bitcoins, the regression theorem, and that curious but unthreatening empirical world**. 27 fev. 2013. Disponível em: <http://konradsgraf.com/blog1/2013/2/27/in-depth-bitcoins-the-regression-theorem-and-that-curious-bu.html>. Acesso em: 22 dez. 2013.

______. **The sound of one bitcoin**: Tangibility, scarcity, and a "hard-money" checklist, 19 mar. 2013. Disponível em: <http://konradsgraf.com/blog1/2013/3/19/in-depth-the-sound-of-one-bitcoin-tangibility-scarcity-and-a.html>. Acesso em: 22 dez. 2013.

______. **On The Origins Of Bitcoin**. 3 dez. 2013. Disponível em: <http://konradsgraf.squarespace.com/storage/On%20the%20Origins%20of%20Bitcoin%20Graf% Acesso em: 5 dez. 2013.

GURRI, Adam. **Bitcoins, Free Banking, and the Optional Clause**. Ümlaut, 6 mai. 2013. Disponível em: <http://theumlaut.com/2013/05/06/bitcoins-free-banking-and-the-optional-clause/>. Acesso em: 13 dez. 2013.

HAYEK, F. A. **Good Money, Part 2: The Standard**, edited by Stephen Kresge. London: The University of Chicago Press Routledge, 1999.

______. A. **Desestatização do Dinheiro**. São Paulo: Instituto Ludwig von Mises Brasil, 2011.

HEARN, Mike. Bitcoin 2012 London: Mike Hearn. YouTube video, 28:19, publicado por "**QueuePolitely**," 27 set. 2012. Disponível em: <http://www.youtube.com/watch?v=mD4L7xDNCmA>. Acesso em: 13 dez. 2013.

HUERTA DE SOTO, Jesús. **Moeda, crédito bancário e ciclos econômicos**. São Paulo: Instituto Ludwig von Mises Brasil, 2012.

HÜLSMANN, Jörg Guido. **The Ethics of Money Production**. Auburn: Ludwig von Mises Institute, 2008.

KAMINSKY, Dan. I Tried Hacking Bitcoin and I Failed. **Business Insider**, 12 abr. 2013. Disponível em: <http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4>. Acesso em: 13 dez. 2013.

KELLY, Meghan. Fool Me Once: Bitcoin Exchange Mt.Gox Falls after Third DDoS Attack This Month. **VentureBeat**, 21 abr. 2013. Disponível em: <http://venturebeat.com/2013/04/21/mt-gox-ddos/>. Acesso em 14 dez. 2013.

KEYNES, John Maynard. **As Consequências Econômicas da Paz**. Brasília: UnB, 2002.

KIRK, Jeremy. Could the Bitcoin Network Be Used as an Ultrasecure Notary Service? **ComputerWorld**, 23 mai. 2013. Disponível em: <http://www.computerworld.com/s/article/9239513/Could_the_Bitcoin_network_be_used_as_an Acesso em: 13 dez. 2013.

LEE, Timothy B. **An Illustrated History of Bitcoin Crashes**, Forbes, 11 abr. 2013. Disponível em: <http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/>. Acesso em: 13 dez. 2013.

LIU, Alec. A Guide to Bitcoin Mining. **Motherboard**, 2013. Disponível em: <http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600>. Acesso em: 10 dez. 2013.

MALTBY, Emily. **Chargebacks Create Business Headaches**. Wall Street Journal, 10 fev. 2011. Disponível em: <http://online.wsj.com/article/SB10001424052748704698004576104554234202010.html>. Acesso em: 10 dez. 2013.

MATONIS, Jon. **Bitcoin Prevents Monetary Tyranny**, Forbes, 4 abr. 2012. Disponível em: <http://www.forbes.com/sites/jonmatonis/2012/10/04/bitcoin-prevents-monetary-tyranny/>. Acesso em: 15 mai. 2013.

______. **Bitcoin's Promise in Argentina**. Forbes, 27 abr. 2013. Disponível em: <http://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/>. Acesso em: 12 dez. 2013.

______. **How Cryptocurrencies Could Upend Banks' Monetary Role**. The Monetary Future, 15 mar. 2013. Disponível em: <http://themonetaryfuture.blogspot.com.br/2013/03/how-cryptocurrencies-could-upend-banks.html>. Acesso em: 22 dez. 2013.

MEIRA PENNA, J.O. de. **Em berço esplêndido** – ensaios de psicologia coletiva brasileira. Rio de Janeiro: Topbooks, 1999.

MENGER, Carl. **On the Origins of Money**. Economic Journal, 1892. pp. 239-255.

______. **Principles of Economics**. Traduzido por James Dingwall e Bert Hoselitz, Free Press of Glencoe, Illinois, 1950; e New York University Press, Nova York 1981.

MIERS, Ian et al. **Zerocoin**: Anonymous Distributed E-Cash from Bitcoin, working paper, the Johns Hopkins University Department of Computer Science, Baltimore, MD, 2013. Disponível em: <http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf>. Acesso em: 13 dez. 2013.

MISES, Ludwig von. **Theorie des Geldes und Umlaufsmittel**. Munique: Verlag von Duncker & Humblot, 1924.

______. **The Theory of Money and Credit**. New Haven: Yale University Press, 1953. p. 462.

______. **A verdade sobre a inflação**. Instituto Ludwig von Mises Brasil, 27 mai. 2008. Disponível em: <http://mises.org.br/Article.aspx?id=101>. Acesso em: 16 dez. 2013.

______. **Ação Humana**: Um Tratado de Economia. São Paulo: Instituto Ludwig von Mises Brasil, 2010.

______. **On Money and inflation** – A Synthesis of Several Lectures. Auburn: Ludwig von Mises Institute, 2010.

NAKAMOTO, Satoshi. **Bitcoin**: a Peer-to-Peer Electronic Cash System, 2008. Disponível em: <http://article.gmane.org/gmane.comp.encryption.general/12588/>. Acesso em: 20 dez. 2013.

OBER, KATZENBEISSER e HAMACHER. Structure and Anonymity of the Bitcoin Transaction Graph. **Future Internet** 5, no. 2, 2013. Disponível em: <http://www.mdpi.com/1999-5903/5/2/237>. Acesso em: 10 dez. 2013.

PAUL, Andrew. Is Bitcoin the Next Generation of Online Payments? **Yahoo! Small Business Advisor**, 24 mai. 2013. Disponível em: <http://smallbusiness.yahoo.com/advisor/bitcoin-next-generation-online-payments-213922448--finance.html>. Acesso em: 11 dez. 2013.

PIERRE. **The Bitcoin Central Bank's Perfect Monetary Policy**. The Mises Circle, 15 dez. 2013. Disponível em: <http://themisescircle.org/blog/2013/12/15/the-bitcoin-central-banks-perfect-monetary-policy/>. Acesso em: 27 dez. 2013.

PINAR ARDIC, HEIMANN e MYLENKO. **Access to Financial Services and the Financial Inclusion Agenda around the World**. Policy Research Working Paper, World Bank Financial and Private Sector Development Consultative Group to Assist the Poor, 2011. Disponível em: <https://openknowledge.worldbank.org/bitstream/handle/10986/3310/WPS5537.pdf>. Acesso em: 12 dez. 2013.

REISMAN, George. **Deflação, prosperidade e padrão-ouro**. Instituto Ludwig von Mises Brasil, 16 ago. 2010. Disponível em: <http://mises.org.br/article.aspx?id=752>. Acesso em: 25 dez. 2013.

RICKARDS, James. **Currency Wars**. New York: Penguin, 2011.

ROTHBARD, Murray N. **The Case for a 100 Percent Gold Dollar**. The Ludwig von Mises Institute, Auburn University, Alabama, 1991.

_____. **Economic Thought before Adam Smith**: An Austrian Perspective on the History of Economic Thought. v. 1, Edward Elgar, Aldershot, Inglaterra, 1995 (Edição espanhola, Unión Editorial, Madri 1999).

_____. **Classical Economics**: An Austrian Perspective on

the History of Economic Thought, vol. II, Edward Elgar, Aldershot, Inglaterra, 1995 (Edição espanhola, Unión Editorial, Madri 2000).

_____. **Man, Economy and State with Power and Market**. Auburn: Ludwig von Mises Institute, 2004.

_____. **O que o governo fez com o nosso dinheiro?** São Paulo: Instituto Ludwig von Mises Brasil, 2013.

RUSSO, Camila. **Bitcoin Dreams Endure to Savers Crushed by CPI: Argentina Credit**. Bloomberg, 16 abr. 2013. Disponível em: <http://www.bloomberg.com/news/2013-04-16/bitcoin-dreams-endure-to-savers-crushed-by-cpi-argentina-credit.html>. Acesso em: 12 dez. 2013.

SALMON, Felix. **The Bitcoin Bubble and the Future of Currency**. Medium, 3 abr. 2013.

Disponível em: <https://medium.com/money-banking/2b5ef79482cb>. Acesso em: 13 dez. 2013.

SCHLICHTER, Detlev. **Paper Money Collapse** – the folly of elastic money and the coming monetary breakdown. New Jersey: John Wiley & Sons, 2011.

SENNHOLZ, H.F. **Money and Freedom**. Spring Mills: Libertarian Press, 1985.

SHOSTAK, Frank. **The Bitcoin Money Myth. Mises Daily**. Auburn: Ludwig von Mises Institute, 17 abr. 2013. Disponível em: <http://mises.org/daily/6411/The-Bitcoin-Money-Myth>. Acesso em: 22 dez. 2013.

SPARSHOTT, Jeffrey. **Bitcoin Exchange Makes Apparent Move to Play by U.S. Money-Laundering Rules**. Wall Street Journal, 28 jun. 2013. Disponível em: <http://online.wsj.com/article/SB10001424127887323873904578574000957464468.html>. Acesso em: 14 dez. 2013.

SPAVEN, Emily. **Kipochi launches M-Pesa Integrated Bitcoin Wallet in Africa**. CoinDesk, 19 jul. 2013. Disponível em: <http://www.coindesk.com/kipochi-launches-m-pesa-integrated-bitcoin-wallet-in-africa/>. Acesso em 12 dez. 2013.

ŠURDA, Peter. **Economics of Bitcoin**: is Bitcoin an alternative to fiat currencies and gold? Diploma Thesis, Wirtschaftsuniversität Wien, 2012. Disponível em: <http://dev.economicsofbitcoin.com/mastersthesis/mastersthesis-surda-2012-11-19b.pdf>. Acesso em: 15 abr. 2013.

TINDELL, Ken. Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995. **Business Insider**, 5 abr. 2013. Disponível em: <http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4>. Acesso em: 10 dez. 2013.

Triennial Central Bank Survey of foreign exchange and derivatives market activity in 2013. Disponível em: <http://www.bis.org/publ/rpfx13fx.pdf>. Acesso em: 10 jan. 2014.

TUCKER e KINSELLA. **Goods, Scarce and Nonscarce**. Mises Daily, Auburn: Ludwig von Mises Institute, 25 ago. 2010. Disponível em: <http://mises.org/daily/4630/>. Acesso em: 22 dez. 2013.

ULRICH, Fernando. Uma semana histórica para o Bitcoin. **InfoMoney**, 13 jan. 2014. Disponível em: <http://www.infomoney.com.br/blogs/moeda-na-era-digital/post/3143266/uma-semana-historica-para-bitcoin>. Acesso em: 13 jan. 2013.

WARREN, Jonathan. **Bitmessage**: A Peer-to-Peer Message Authentication and Delivery System, white paper, 27 nov. 2012. Disponível em: <https://bitmessage.org/bitmessage.pdf>. Acesso em: 13 dez. 2013.

WILLETT, J. R. **The Second Bitcoin Whitepaper**. White paper, 2013. Disponível em: <https://sites.google.com/site/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf>. Acesso em: 13 dez. 2013.

WOLF, Brett. Senators Seek Crackdown on ‘Bitcoin’ Currency. **Reuters**, 8 jun. 2011. Disponível em: <http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608>. Acesso em: 14 dez. 2013.

WOODS Jr., Thomas E. **Meltdown**. Washington: Regnery Publishing, 2009.

World Bank Payment Systems Development Group, **Remittance Prices Worldwide**: An Analysis of Trends in the Average Total Cost of Migrant Remittance Services. Washington, DC, World Bank, 2013. Disponível em: <http://remittanceprices.worldbank.org/~/media/FPDKM/Remittances/Documents/RemittancePri Analysis-Mar2013.pdf>. Acesso em: 11 dez. 2013.

YUNUS, Muhammad. **Banker to the Poor**: Micro-lending and the Battle against World Poverty. New York: Public Affairs, 2003.